

SHIELDX OVERVIEW

Q: What is ShieldX? What does it do?

A: ShieldX is a 100% software, network-based security platform for protection of core business infrastructure services that span across multiple physical, virtual and cloud-based environments or the “multi-cloud”. It offers fully scalable and automated visibility, microsegmentation, and threat and malware detection and prevention to support security policy creation, enforcement and compliance.

Q: Who are the primary users of ShieldX?

A: ShieldX is ideally suited for deployment by the cloud and infrastructure, security and DevOps teams within enterprise, service provider and professional services organizations.

Q: Is ShieldX a product or a service?

A: While ShieldX follows cloud-principles regarding elasticity, automation, and the economics of lower resource costs and on-demand deployment, ShieldX is actually a software-based product. It is not what is known as a “Security-as-a-Service” or “managed service” model. ShieldX does not host your deployment, or manage it for you. We just make it easier for you. Organizations acquire, deploy and manage it within their infrastructure, whether on-premises, hosted, within public cloud or combinations of all of it.

Q: Is ShieldX a “cloud security”, or a Cloud Access Security Broker (CASB), solution?

A: ShieldX does secure clouds deployed by our customers. But unlike CASB solutions that secure

communications between users and external environments and services like SaaS, ShieldX focuses on securing the network traffic within the organization as part of its critical infrastructure — whether in data centers or in hosted, colo and/or public cloud services. We call it “multi-cloud” security because of its inherent ability to traverse all varieties of cloud architectures, virtualized infrastructure and even physical environments.

Q: Is ShieldX a Cloud Workload Protection Platform (CWPP)?

A: We protect workloads but through a network vs agent/endpoint approach. According to Gartner’s definition, CWPPs offer endpoint-based protection. ShieldX is a network-based security solution, providing security controls generally categorized as network, content and Data Loss (or Leak) Prevention* (DLP) security. In addition, ShieldX does not install software/agents onto any of the workloads that it protects.

Q: ShieldX sounds a lot like a Next Generation Firewall (NGFW.) Does it replace them?

A: ShieldX does offer many of the same security controls as a NGFW including ACLs, application classification and intrusion prevention. But ShieldX isn’t intended to replace the physical, appliance-based firewalls at the perimeter of a data center. ShieldX is designed to complement these solutions and the customer investments they represent.

However, ShieldX is an ideal, cost-effective replacement for NGFW virtual appliances. Traditional virtual appliances exact a high tax on deployment

within the data center or the cloud when considering performance, licensing and infrastructure costs. They also present challenges in efficient operations, scale and security management.

Q: What are the most common ways ShieldX may be deployed and used?

A: While the ShieldX platform and its modularity render it capable of many use cases, our customers tell us it is ideally suited to:

- Secure on-premises infrastructure — Segment and secure lateral, “East-West” traffic across virtualized and orchestrated private clouds and data centers – especially if there is a mix of new and legacy technologies, and compliance is a concern.
- Secure public clouds — Segment and secure within and at the perimeter of public cloud deployments, especially where there is a need for high performance and cost control.
- Secure a multi-cloud environment — Create, automate and enforce uniform security policy across disparate environments.
- Enable Managed Security Services & Providers — Remotely deploy, manage and monitor infrastructure security, including within OpEx-based engagement models.
- Secure IP Transport Providers — Offer “Clean Pipe” connections at scale and on-demand according to current requirements, need and subscriber requirements.
- Empower DevOps — DevOps teams can work with ShieldX to integrate with and secure new applications and environments. Or, security and operations teams can use ShieldX for a DevSecOps style of security operations management. The ShieldX API-First strategy allows for all of its capabilities to be dynamically controlled via RESTful APIs.

SHIELDX ARCHITECTURE

Q: Is ShieldX an appliance? Where does it install? Does it come with hardware?

A: ShieldX is the anti-appliance. Appliances, whether physical or virtual, are based on converged, monolithic software that is typically designed to run on custom, proprietary hardware in order to maintain performance with a full set of security features enabled.

ShieldX runs on your commodity hardware and hypervisors as a distributed, microservices-based architecture. It shares the same infrastructure resources as the services it protects, so it is up to you to determine how much investment and how many resources you wish to allow security services to consume. And it will only use them as you need them, freeing up resources for your core business services.

Q: What is a “microservices-based architecture”?

A: Known to the world of application developers and DevOps teams, a microservices-based architecture is an application model that deconstructs traditional, monolithic software into its component parts, and then distributes and chains them. This allows dynamic replication and scale of each component as needed, rather than having to replicate the entire code set when just one function fails to scale, or simply, fails.

Q: ShieldX is “containerized”. What exactly does that mean and why does it matter?

A: Each of the ShieldX microservices, or xServices, is packaged into a container to offer a lightweight footprint, reliability, scale and non-disruptive upgrades. These containers are then “wrapped” in a virtualized form factor that allows them to be deployed into the environments requiring protection, such as VMware vSphere®, AWS EC2® or Microsoft Azure®.

Q: What does ShieldX “unlimited scale” and “uncompromised security” really mean? And could it eat my network?

A: Due to its 100% software, microservices-based architecture, ShieldX scale is limited only by the infrastructure resources allocated to support it. It will grow with your network, its traffic and its security needs — even with deep packet inspection and TLS decryption/re-encryption fully enabled, which are both resource intensive services.

In addition, ShieldX is built to serve and protect core business critical services, not displace them. Its active, self-orchestration functions continually monitor infrastructure utilization to ensure it doesn't overrun your hosts or networks.

SHIELDX COMPATIBILITY

Q: Which environments is ShieldX compatible with?

A: The ShieldX architecture is designed to quickly integrate with most environments. Version 1.2 supports VMware vSphere™ 5.5-6.0 and AWS EC2® and Microsoft Azure® environments. Please refer to www.ShieldX.com for more information and inquiries.

Q: ShieldX runs over “commodity hardware” or “infrastructure”. Which chipsets or hardware platforms does ShieldX support?

A: ShieldX is currently optimized for operation over Intel® Xeon® CPUs (Sandy Bridge or later.)

Q: ShieldX lists partnerships with other companies. Is ShieldX certified with any of these environments?

A: ShieldX is certified VMware-Ready® and OpenStack Compatible®. We are partnering with multiple vendors and will be updating our certification list soon. Please contact us at www.ShieldX.com if you have any questions.

Q: Can ShieldX integrate with other security products?

A: ShieldX currently integrates with FireEye® AX appliances and Helix Cloud. IT teams and their

providers may also use our REST-based APIs and syslog export to create custom integration with other systems, like SIEMs.

Q: Can we customize ShieldX or access and control it via API?

A: Yes. Everything that can be done through the management console (and more) can be accessed and controlled via RESTful API.

Q: Can ShieldX import more intelligence feeds? Where does its intelligence come from?

A: ShieldX uses and embeds third-party intelligence feeds from market-leading providers. These feeds pair with the intelligence ShieldX gains through its discovery and profiling analytics to provide a tailored combination of community knowledge with intel that is automatically customized to your environment.

In addition, to support an industry best practice of leveraging community intel, ShieldX can import additional feeds you may already subscribe to. Please contact us at www.ShieldX.com if you have questions and are interested in assistance in configuring this capability for your deployment.

DEPLOYING SHIELDX

Q: How can we estimate and effectively size the supporting hardware infrastructure that ShieldX needs to operate?

A: ShieldX offers resource requirement tables per each supported environment to help your team estimate the resources ShieldX will consume, based on how much traffic you will inspect (with or without TLS decryption). If you are uncertain of your traffic volume and trends, you can ask us for guidance, evaluate ShieldX for a snapshot, and/or start with a base configuration with the freedom to upgrade as needed without penalty.

Q: Is ShieldX deployment disruptive? Does it require shutdown of the network or its services to deploy for the first time?

A: Not at all. And this is a defining difference between ShieldX and other solutions on the market which require network shutdown, image edits/reloads, or manual (and ongoing) reconfigurations of the service chain.

ShieldX inserts transparently into each network you have configured it to secure using the credentials you have provided. It automatically discovers the details it needs to use to work within each environment, freeing valuable security architect and analyst time to focus on strategic security policy creation, process and investigations.

Q: How do we upgrade ShieldX? Does it require a rip-and-replace upgrade process?

A: Due to its microservices-based architecture, ShieldX is designed to inherently support high availability and non-disruptive update, patch and removal. Updates/upgrades will be downloadable as they become available.

Q: ShieldX is a security product. But as a containerized, microservices platform, does deploying it introduce new vulnerability into my network?

A: ShieldX is a team of security experts. We've taken special care to employ best practices in the development of our product, following guidelines of the SSDLC, using leading test and code analysis tools, and employing concepts such as "defense in depth" and the "principle of least privilege." We also use ShieldX in our own production IT environment. If you would like to learn more, please contact us at www.ShieldX.com for a briefing.

Q: Where can we learn more about ShieldX security features? And what is an "IoP?"

A: You are always welcome to contact us for product documentation and materials that detail

the capabilities of ShieldX security controls, policy creation, its analytics and yes, IoP.

Indicator-of-Pivot (IoP) is a security feature unique to ShieldX. Unlike the Indicator-of-Compromise (IoC) that typically represents volumes of perimeter-based alerts and contributes to time-consuming or distracting false positives, ShieldX uses real-time analytics to identify lateral movement by attackers, reduce actions on false positives, and helps security analysts start tracking threats earlier and throughout the entire Cyber Kill Chain.

GETTING SHIELDX

Q: Is ShieldX available now?

A: Yes. ShieldX is available now. Customers and Partners may engage with ShieldX today at www.ShieldX.com for a briefing and demonstration, and to run a Proof-of-Value evaluation.

HOW IS SHIELDX LICENSED?

Q: ShieldX is designed to offer the agility and flexibility IT organizations expect of Cloud-native solutions.

A: ShieldX is offered in a capacity based license model, beginning at 10 Gbps of security inspection, with incremental upgrades of 2 Gbps as needed. Primarily sold as a subscription, for simplicity, our support contract is now included.

ShieldX is also available in consumption based models for public clouds.

Q: Do we buy a separate ShieldX license for every environment we will run it in?

A: No. ShieldX offers an "all you can eat" model. You can use all of its security controls, in any supported environment, and for as many data planes and

microservices as you need. The ShieldX license is tied to a single Virtual Chassis defined by a single management plane. If you decide to buy more than one license, it will be due to your unique business and operational requirements, and not for any lack of scale or separation of duties in ShieldX.

Q: How do we get support for ShieldX?

A: When evaluating ShieldX, our presales team is available to assist with your questions and your proof-of-value deployment.

ShieldX customers are entitled to premium, 24x7 support and updates online and by phone.

Whether evaluating or actively using ShieldX to secure your environment, you may request access to our Customer + Partner Portal for product downloads, documentation, training, and our knowledgebase.

Q: Can we evaluate ShieldX?

A: Absolutely. In fact, we encourage you to evaluate it thoroughly and compare it to other solutions on the market. Contact ShieldX at www.ShieldX.com to request an evaluation.

Q: How do we right-size our ShieldX license purchase? And can we upgrade later?

A: This is where evaluation can help. While you may have some estimations of your traffic, ShieldX can help provide visibility into how much traffic is actually traveling across your network – including its peaks

and valleys. And you will not be penalized for starting low and upgrading later as you gain more insight, or your requirements change.

Q: Our company has a defined purchase process and approved vendor and supplier list. Can you work with our process and approved list?

A: Yes. ShieldX can work with your process and your vendors and Providers. If your preferred Provider is not already engaged with us, please provide us their contact information, or direct them to contact us through our website at www.ShieldX.com.

Q: What does ShieldX mean by “unparalleled economics?”

A: ShieldX fully embraces cloud principles – the ability to access and pay for what you need or consume, when you need it, with cost-effective prices and flexible business models.

Enabled by its elastic architecture, ShieldX offers lower TCO and helps reduce operations costs of licensing, hosting/services, infrastructure, staff, and maintaining SLAs. If you would like to hear more details on our business case, please contact us at www.ShieldX.com for a briefing.