SHIELDX

ShieldX™ Security Controls and Features-Quick Reference

FOCUS: SHIELDX SECURITY CONTROLS AND FEATURES-QUICK REFERENCE

ShieldX's rich set of security controls and security features are enforced by every in line and/or microsegmentation data plane deployment This document references the security controls and features available in the latest release.

Firewall

An Access control policy is an ordered set of rules that govern the ability of data center workloads to permit or deny connections. ShieldX also offers ACLs with APP-ID. ShieldX ACLs are enforced across multi-cloud infrastructures and are an integral part of ShieldX microsegmentation insertions that allow ACLs to be applied even between workloads on the same infrastructure subnet. ShieldX is used as a more cost effective and scalable option to replace virtual firewalls.

Application Anomaly Detection

ShieldX anomaly detection works in concert with ShieldX Deep Packet Inspection (DPI) as part of insertion and continuous monitoring via Segment Interfaces (Sis) or Flow Inspectors (Fis). Anomaly Detection is a configuration-based detection engine that uses its own content to detect brute-force logins (src and dst are the same, time bound); host scannings (dst, range of ports, time bound); network scannings (range of dst, fixed ports, time bound); App/DOS (same alert is fired over a threshold, dst, time bound); high-volume data transfers (src, dst, src port, dst port are same, time bound); traffic transfers on non-standard ports (dst, dst port); any unusually low data transfers (src, dst, src port, dst port are same, time bound); a high volume of attacks on the same source (time bound); Layer 7 reconnaissance (available in an upcoming release); post exploit behavior change (an exploit was detected that resulted in change in behavior of an application); and Machine Learning-based anomalies (assessed via feedback from the larger ShieldX system and used to track network behavior patterns, variants and anomalies. Anomaly Detection includes alerting of application threats and/or vulnerability-breaches.

Threat Prevention I Intrusion Prevention Policy

ShieldX Threat Prevention Policy uses a third-generation DPI engine for speed and accuracy with full protocol parsing for applications and threats via a set of rules that detect exploit attacks and policy viotio11s, including the actions to take when threats are detected. Based on an aggregate of threat signatures and the parsing of over 100 protocols, ShieldX IPS identifies threats regardless of the protocol(s) state [for example, an HTTP request protocol (such as GET, PUT, etc) is inspected as thoroughly as the HTTP response phase of the protocol]. In fact, ShieldX Threat Prevention employs one parse machine per protocol- a protocol parser for every protocol it decodes and inspects. In addition, ShieldX automatically selects the right protocol to inspect, irrespective of port - for example, if HTTP is run on port 80 but a customer is running HTTP on 8080, ShieldX identifies and applies the right protocol parsing and threat detection logic to HTTP on port 8080 without user configuration. With ShieldX application classification, ShieldX also uses its understanding of application operations to parse the protocol and decipher an application (detect an application); this enables users to write threat prevention policies using the name of that discovered application, with threat rules defi1led per application (ShieldX IOP will also recommend policies for discovered applications i1 an upcoming release). Lastly, ShieldX uses threat intelligence from multiple feeds, updated every two weeks, to write its threat detection rules [obtained from IDAPPCOM and TrendMicro (formerly TELUS), and from WEBROOT for URL filte ring, and FIREEYE for integrated sandboxing and behavioral analysis.

Malware Policy and Network Object Extraction (NOX) Blocking

ShieldX Malware Policy is a set of rules that drive traffic inspection and response actions when malware is detected, including forwarding of the malware to a third party system for further behavioral analysis via sandboxing. In addition, the ShieldX Network Object Extractor Service performs inline NOX Blocking in data planes, in concert with the DPI microservice and assigned malware policy -detecting suspicious files in cache or cloud, blocking, alerting on, and forwarding to enabled malware engine(s), including the ShieldX Cloud and/or Fire Eye appliances (or Fire-Eye Cloud). NOX Blocking includes in line scanning of a specified file or protocol (HTTP, SMB, SMTP) that returns a level of confidence scoring (High or Clean) with regard to the maliciousness of the file, in addition to other details about file and behavioral analysis results from malware analysis. ShieldX provides both detection and blocking capabilities for NOX. ShieldX Maware Policy includes URL classification and reputation lookup, and all file types are sandboxed for analysis for malware detection.

Indicator of Pivot (IOP) Isometric Infrastructure Visualizations, Correlations and Lateral Detections

ShieldX IOP tracks malicious attempts to move malware in East/West traffic (laterally) inside a data center or cloud after the North/South boundary has been breached. ShieldX detects indicators of pivot and provides correlation data for analysis. ShieldX IOP visualizes real-time analytics from its own continuous multi-cloud discovery and enhanced DLP monitoring systems to automatically identify lateral attacks that move and pivot across clouds and data centers. Using a rich set of security controls enabled by ShieldX flow (FI) and segment interface (SI) inspectors, IOP technology correlates flow and network events with all the various ShieldX detection engines and controls to provide security analysts with actionable intelligence and a detailed visual and interactive investigative toolkit.

Data in Motion (DIM) Detection

ShieldX DIM and DLP engines also work in concert to monitor flows and protocols (HTTP, SMB, SMTP, POP3, etc) to dete ct regulatory and sensitive data (like PII, PCI, HIPAA) as it moves in infrastructures. The DLP Engine fingerprints data in motion to identify any regulatory violations in flows, and if violations are detected, ShieldX compares with known vulnerabilities that might be exploited by an attacker while IOP maps potential exfiltration targets (hops). Events from DLP are sent to IOP for tracking data exfiltration. Regulatory patterns are updated every two weeks from the ShieldX SXTI Cloud. And inspection and tracking of data at rest is available in an upcoming release.

URL Filtering

URL Filtering Policy is a traffic threat detection feature that operates in concert with the ShieldX SXTI Cloud service. When an URL Filtering policy is configured, the ShieldX data plane sends real time URL filtering queries to the local SXTI Cloud service, which is continuously managing security content updates.

ShieldX URL classification and reputation includes parsers that extract domains and URLs from HTTP, HTTPS and DNS, in addition to URL and domain reputation configurability (sliders), and the option to allow or deny classes of URLs. Moreover, customers can create their own custom classes (lists) of URLs.

Security Policy Sets

Security contro ls can be grouped by the ShieldX administrator into Security Policy Sets (SPS), then applied to and binded to object groups of workloads/CID Rs, selected networks or machine-learning objects. An SPS is assigned to an ACL per Data Plane Access Control Rule.

TLS De-encryption; Flow Inspector with TLS (FIT) [for Azure and AWS environments]

The ShieldX Transport Layer Security (TLS) Service de-/re-encrypts connections for continuous inspection using TLS protocol parsing for protocol vulnerability detection, then terminates detected threats. ShieldX TLS Policies are applied to ACLs across infrastructures in multi-cloud environments, and supports both inbound and outbound decryption, acting as a transparent proxy (without IP configuration). ShieldX TLS Inbound proxy needs private keys, and the Outbound proxy requires clients to trust a root CA (either ShieldX's or the customer's root CA). ShieldX TLS uses SNI Domain Reputation database for domain reputation, and Certificate Blacklist for bad certificates used by attackers. The new TLS protocol version 1.3 is fully supported by ShieldX.

Global Threat Configuration

Data centers and clouds can contain tens of thousands of networks and workloads. ShieldX ‘s Global Threats Configurations page allow an admin to modify settings that will take affect across all policies. Use this security feature to adjust status settings and apply log, alert, blocking, email notifications and syslog generation parameters to “All” or a subset of threat rules or threat detections.

Whitelisting and Blacklisting

Use the ShieldX White/Blacklists options to define, import or export a Custom URL Category for whitelisting or blacklisting. You can also configure IP Blacklisting [using X-Forwarded-For (XFF) HTTP Header Client IPs].

Auto-Insertion of Segment Interfaces (Sis) or Flow Inspectors (Fis) for continuous monitoring

A self-generating SI (in VMware environments) or FI (in AWS and Azure environments) microservice that connects itself to a network segment to perform continuous inspection. Each self-inserting SI or FI serves as the entry point for all traffic threat analysis and security control responses in a virtualized data center or 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

November 2018