SHIELDX

ShieldX and the SWIFT CSP

ShieldX's agentless microsegmentation provides Zero Trust security to data centers in AWS, Azure and VMware environments while facilitating compliance, protecting East-West traffic, and delivering visibility, automation and cloud-native controls. By leveraging deep packet inspection (DPI), ShieldX implements threat prevention, virtual patching and fine-grained East-West controls, allowing customers to automatically orchestrate data center security in multi-cloud environments.

WITH SHIELDX, SECURITY TEAMS CAN:

- Visualize multi-cloud deployments and associated risks
- Microsegment flat networks to stop lateral movement and satisfy regulatory requirements
- Automatically secure multi-cloud environments with adaptive security policy
- Lower the cost of security with consolidated controls and deep automation

SHIELDX: SUPPORTING THE SWIFT CSP

The Customer Security Program (CSP) is a new framework launched by the Society for World Interbank Financial Telecommunication (SWIFT). The CSP is a compliance regime and SWIFT will report non-compliant organizations to their regulators and other SWIFT member organizations. ShieldX provides capabilities that enable you to meet CSP requirements.

The CSP can be broken down to three objectives, eight principles, and 27 controls. Of these 27 controls, 16 are mandatory and 11 are so-called "advisory controls." The three objectives are a good summary of exactly what ShieldX does for customers: secure the environment, know and limit access, and detect and respond.

SECURING SWIFT ENVIRONMENTS

Of the eight principles SWIFT's CSP lays out, the first half of them fall under "Secure Your Environment":

- Restrict internet access
- Protect critical systems from general IT environment
- Reduce attack surface and vulnerabilities
- Physically secure the environment

With ShieldX, banks comply with SWIFT by gaining application-level visibility and giving data center workloads access only to the other workloads they need to interact with. Attackers cannot pivot to workloads they cannot see or access, so the system must limit their visibility.

MICROSEGMENTATION ACCESS CONTROLS

Two of the SWIFT CSP controls fall under the rubric "Know and Limit Access":

- Prevent compromise of credentials
- Manage identities and segregate privileges

ShieldX uses microsegmentation and a container-based, microservices architecture to create logical tiers and zones regardless of physical infrastructure. With ShieldX, enterprises can automatically create security zones, logical tiers within each zone,

isolate each tier and zone, and then microsegment tier members. And all this is performed across multiple business applications. In Gartner's **Solution Comparison for Microsegmentation Products** (April 2019), a microsegementation approach based on application logic:

- Helps the security of distributed applications that are not segregated into traditional tiers
- Is the basis of AI/ML-based capabilities for policy building. AI/ML-based capabilities create draft policies and templates based on the application logic that they learn

ShieldX uses machine learning to discover workloads and automatically generate microsegmentation security policy in multi-cloud environments. Finally, ShieldX automatically transforms proposed policies into advanced security controls. Connectivity is allowed (or not) based on security policies that express business requirements, and are not simply gated by IP addresses (via an access control list, or ACL).

FULL DEEP-PACKET INSPECTION

The remaining two CSP controls fall under "Detect and Respond":

- Detect anomalous activity to the system or transaction records
- Plan for incident response and information sharing

ShieldX offers full deep packet inspection (DPI). True to it's cloud-native approach, ShieldX implements its microservices components using containers—meaning services are scaled with high granularity. If DPI reaches a maximum load, a new instance of that specific service alone can be launched, as opposed to a transplanted traditional zone approach, where an entire appliance-based firewall virtual appliance must be used. Moreover, a full set of API's allows automation and orchestration of policies and controls.

VIRTUAL PATCHING FOR AUTOMATED VULNERABILITY MANAGEMENT

When it comes to "detecting and responding," virtual patching is a critical part of any current defense posture. You can use a vulnerability scanner to find problems in your network and then, in theory, you could take the scanner report and use a team of experts to manually generate the policies needed to provide virtual patches. But the expense and time intensity of this process is formidable: there are too many patches and too many (dynamic) workloads. According to Gartner, a "vulnerability remediation prioritization catalog is a big task to undertake with manual labor and this is a key reason few have ever attempted this, let alone completed it."

With ShieldX, you can use a best-of-breed vulnerability scanner and then ShieldX will generate network-based virtual patching policies. Furthermore, ShieldX includes the unique capability of applying a virtual patch solely to workloads that are running the application that is vulnerable to a specific attack. The ShieldX virtual patch may be applied as soon as the vulnerability is detected, but the per-workload application of the virtual patch means that there are radically lower chances of a false positives.

SWIFT CSP AND SHIELDX

SWIFT's motive in creating the CSP is to provide a framework for security at financial institutions in a way that provides individual organizations the flexibility to implement the mandatory and additional advisory controls in ways that best suit their organizations. Organizations can try to add on-point solutions that passively monitor for network intrusions, for example. Or they can engage architectures and methodologies that deliver organically robust security at the level of workload-to-workload interactions.

MANDATORY SECURITY CONTROLS	CONTROL OBJECTIVE	SHIELDX CAPABILITY
1. Restrict Internet Access & Protect Critical Systems from General IT Environment		
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	The intent behind Requirement 2 is to implement sufficient preventive controls to reduce the attack surface. These controls include changing vendor passwords; enabling only necessary services, protocols and daemons; and removing unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and web servers. For a relatively complex cardholder data environment, there are potentially thousands of instances in which unnecessary services, unnecessary functionality, and insecure services could operate. ShieldX ESP leverages deep packet inspection and integration with leading vulnerability management solutions to detect threats targeting your systems containing sensitive PCI data. Our patented technology inspects content as it traverses the network, identifying ports, protocols and applications.
2. Reduce Attack Surface and Vulnerabilities		
2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	ShieldX supports software updates and can content updates to minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure. Also, ShieldX can also provide virtual patching for SWIFT infrastructure.

2. 3 System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.	ShieldX supports system hardening, by locking down unused ports, protecting systems from threats, applying microsegmentation to reduce cyber attack surface of SWIFT-related components.
2.7 Vulnerability Scanning*	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.	ShieldX supports Vulnerability scanner integration such as Rapid7 insightVM to identify known vulnerabilities within the local SWIFT environment and act upon scanning results accordingly. ShieldX also offers microsegemenation and virtual patching as comp control.
6. Detect Anomalous Activity to Systems or Transaction Records		
6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.	ShieldX can proactively protect workflows across the multicloud using a combination of static and dynamic inspection, either on-premise or in the cloud to offer malware protection.
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	ShieldX supports rich set of logging and monitoring includes detecting amonalous actions and operations and recording security events. ShieldX also has its own anomaly detection engine with statistical as well as machine learning capabilitites, syslog forwarding is also possible.
7. Plan for Incident Response and Information Sharing		

7.1 Cyber Incident Response Planning	Validate the operational security configuration and identify security gaps by performing penetration testing.	
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.	ShieldX offers security training, awareness activities and professional services to ensure all staff are aware of and fulfill their security responsibilities.

ADVISORY SECURITY CONTROLS	CONTROL OBJECTIVE	SHIELDX CAPABILITY
1. Restrict Internet Access & Protect Critical Systems from General IT Environment		
1.3A Virtualisation Platform Protection*	Secure virtualisation platform and virtual machines (VM's) hosting SWIFT related components to the same level as physical systems.	ShieldX offers security training, awareness activities and professional services to ensure all staff are aware of and fulfill their security responsibilities.
2. Reduce Attack Surface and Vulnerabilities		

2.4A Back Office Data Flow Security	Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.	ShieldX offers granular security controls with optimal segementation and logical zoning and can ensure confidentiality, integrity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components. ShieldX supports microsegmentation, threat prevention, TLS decryption and other security controls.
2.8A Critical Activity Outsourcing	Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	ShieldX offers granular security controls with optimal segementation and can restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business. Also, ACLs and groups can be set up to achieve this.
2.9A Transaction Business Controls	Restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business.	ShieldX offers granular security controls with optimal segementation and can restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business. Also, ACLs and groups can be set up to achieve this.
2.10A Application Hardening*	Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-certified messaging and communication interfaces and related applications.	ShieldX also offers microsegemenation and virtual patching as comp control.
5. Manage Identities and Segregate Privileges		

5.3A Personnel Vetting Process	Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.	N/A
6. Detect Anomalous Activity to Systems or Transaction Records		
6.5A Intrusion Detection	Detect and prevent anomalous network activity into and within the local SWIFT environment.	
7. Plan for Incident Response and Information Sharing		
7.3A Penetration Testing	Validate the operational security configuration and identify security gaps by performing penetration testing.	N/A
7.4A Scenario Risk Assessment	Evaluate the risk and readiness of the organization based on plausible cyber attack scenarios.	ShieldX has large set of customer deployments and ShieldX evaluate the risk and readiness of the organization based on plausible cyber attack scenarios. Also, Shieldx helps visualize corporate risk in various ways, for example: flat networks, vulnerabilities and sensitive data movement using ShieldX's patented Indicator of Pivot technology. This drives security policy for better cyber defense.

* new advisory controls

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

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