SHIELDX

CISO’s Guide to ShieldX and Zero Trust Networking

With the onset of cloud computing, perimeters dissolved due to fragmented data centers. Suddenly, data and applications went from nicely confined rooms with a handful of doors and windows to virtualized environments with no perimeters. It was back to the Wild West, which meant security and compliance were quickly downgraded—and the increased interest in Zero Trust for network security. In fact, NIST has released Draft Special Publication (SP) 800-207, Zero Trust Architecture. Forrester’s report, **Zero Trust For Compliance** (July 15, 2019), details control mapping for Zero Trust against 12 industry and government compliance mandates.

Historically, security was attempted primarily by fortifying the data center perimeter. That architecture is no longer effective, as there is an incongruity between the physical datacenter boundary and virtual perimeters. Those new perimeters can take up any size and shape and change at cloud speeds, making it impossible for traditional security to follow. Additionally, the security controls offered by cloud vendors are weaker than traditional options and are often no match against attacks hindering confidence and compliance in cloud adoption. A comprehensive Zero Trust networking architecture is required.

Today, many vendors tackle the problem with agents, rigid rule-sets or hard coded approaches. Inevitably, you’ll be let down in your cloud migration journey if you deploy any of these options — with negative repercussions on compliance, security and cost. Many early adopters of agent-based approaches already regret their decision.

WHAT IS ZERO TRUST NETWORKING?

Creating a Zero Trust networking architecture means creating a least privileged environment. This requires an understanding of:

- N-tier application structure
- Tier boundaries
- Tier isolation
- Microsegmentation
- User, process and workload identity
- Threat prevention
- Virtual patching

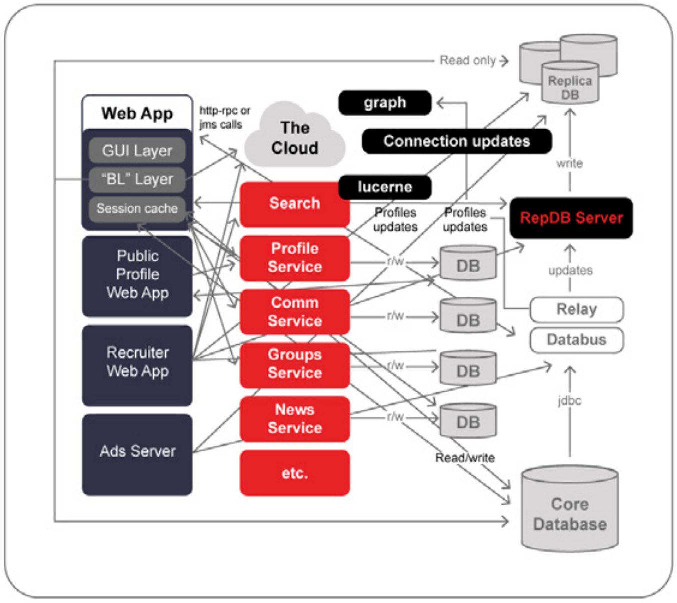
SHIELDX AND ZERO TRUST NETWORKING

The ShieldX Elastic Security Platform was built to secure modern, multi-cloud data centers. ShieldX brings:

- Application level visibility
- Automated network security policy
- Automated threat prevention security policies
- Automated control deployment

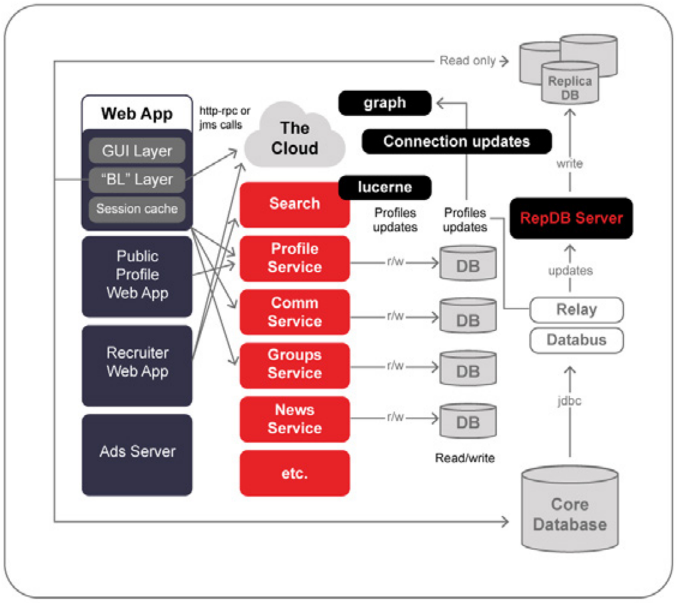
TODAY, THE BIGGEST OBSTACLES TO DEPLOYING ZERO TRUSTNETWORK ARCHITECTURE ARE:

Security teams do not understand application architectures. Networks are built with inherently liberal zoning strategies. Typically, network zones equate to a VLAN that hosts the full set of application tiers—all web servers of all applications in the same VLAN. Also, inter-VLAN isolation rules are not established. For example, a web server VLAN can talk with any other VLAN with impunity because the security does not know what restrictions to impose. A confusing, complicated “architecture” as depicted here:



SHIELDX: ENABLING ZERO TRUST NETWORKING

Agentless microsegmentation brings visibility, automation and cloud-native controls to secure East-West traffic, facilitates compliance, and enables Zero Trust for data centers in AWS, Azure and VMWare. By leveraging deep packet inspection, ShieldX delivers threat prevention and fine grained East-West controls, allowing customers to automatically orchestrate data center security in multi-cloud environments.



ShieldX dynamically scales to deliver comprehensive and consistent controls to protect data centers, cloud infrastructures, applications and data— no matter where they are or where they go—to make the cloud more secure than on-premise deployments. This frictionless approach leverages agentless technology as well as the ShieldX Adaptive Intention Engine, which autonomously translates and enforces intention into a set of comprehensive controls—microsegmentation, firewall, IPS and more.

ZERO TRUST NETWORKING CHECKLIST VS SHIELDX

FORRESTER ZERO TRUST RECOMMENDATION	SHIELDX ELASTIC SECURITY PLATFORM ACHIEVEMENTS
Improve network visibility •Inspect all network traffic for malicious activity. •Prevent or limit the damage of data breaches. •Limit the pain of vulnerability management issues.	Upon deployment of the ShieldX Elastic Security platform, the system will automatically uses network logs and deep packet inspection capabilities to detect all resources and their logical connections across VMWare and multi-cloud environments. The connection mapping identifies how systems are interconnected for visibility into potential vulnerabilities, misconfigurations or rogue systems operating within the environment.
Stop Malware Propagation •Prevent malware propagation between critical systems.	Agentless malware sandboxing (static and dynamic analysis available) utilizes deep packet inspection to identify anomalous files, as well as network object extraction, which is responsible for fetching the reputation of the files/data and hence detecting malicious traffic transferred over the network.
Reduce Both Capital and Operational Expenditures on Security •Consolidate multiple, disparate security controls from across the network. •Reduce management costs.	The multi-cloud security platform provides centralized security policy management across on-prem and off-prem (multi-cloud) environments, creating a single, scalable management console for policy, events, analytics, automation and remediation. The automation reduces times and resources utilized to manage and orchestrate security controls across each environment. Additionally, the microservices model of the platform provides a scalable and elastic solution that only utilizes required resources when needed, based on your operational

	needs, thus reducing the overall operating costs in both on-prem and cloud architectures.
Reduce the Scope and Cost of Compliance Initiatives •Reduce the scope of industry regulations. •Ease the pains of compliance audits.	ShieldX supports compliance initiatives by supporting the microsegmentation of flat or segmented networks. The visibility tool built into the ShieldX platform also provides insight into potential misconfigurations and vulnerabilities tied to improper connection rules which are vital to understanding compliance needs.
Eliminate Intersilo Finger-Pointing •Foster close relationships with other technology teams. •Break down interdepartmental silos.	The platform helps bridge the communication gaps between the Dev-Ops team responsible for the deployment of new technologies and the security team tasked with protecting it. It provides both teams with visibility into the infrastructure and the security policies necessary to maintain a secure environment under a single pane of glass.
Increase Data Awareness and Insight •Support Data Privacy Issues •Accurately identify sensitive data	Our sensitive data inspection engine security controls detect leaks using pre-configured rules, alerting security practitioners on potential exfiltration attempts across all environments.
Stop the Exfiltration of Sensitive Data into the Hands of Malicious Actors •Protect the firm’s intellectual property and future revenues. •Protect customers from the emotional and financial toll of a breach.	The platform’s unique Indicator of Pivot capability helps accurately identify sensitive data threat events, and subsequently correlate them with other phases of the Kill Chain to identify data exfiltration attempts. This, in conjunction with the DLP control and proper configuration of S/N perimeter rules, allows ShieldX to protect sensitive data exfiltration from an organization’s environment.

Enable Digital Business Transformation •Become a partner in digital transformation. •Accelerate the adoption of IoT.	By providing automated security controls and application level microsegmentation, the ShieldX elastic security platform enables new services to be rapidly deployed with automatic security controls in place at the microsegmentation level, enabling business operations to thrive and continue without forgoing security and increasing risk to the organization.

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