EDGEWISE
ZERO TRUST SEGMENTATION

DATA SHEET

Edgewise for Container Security

Improve application security, at developer speed

Containerization is quickly becoming the go-to method for application development and deployment, driven by ease and flexibility. Software developers especially like the seamless integration with the CI/CD pipeline, where containerization technologies allow developers to treat infrastructure as code, to write-once, and to easily and rapidly deploy software through a succession of environments.

However, security tops the list of concerns companies have about containerization. That ease of deployment through a succession of environments means that flaws, vulnerabilities, and security risk impacts not just one, but potentially hundreds of services. Existing security has failed to adapt to how modern applications are built, and deployed...until now.

The Edgewise Advantage

Identify and map applications and their network communications

As developers build and deploy software into containerized environments, security tooling must be able to identify its presence and its provenance. Edgewise continuously scans network communication to, from, and within containers, to discover applications and services the moment they attempt to communicate. Once identified, every application is fingerprinted based on immutable identity attributes. This unique identity—a cryptographic definition of the application running within the namespace of a container—governs all access to network resources, both within and beyond the container.

Enforce application-aware policies

Edgewise's application-aware approach to policy creation decouples security from the network and results in hardened policies that are portable across instances and environments. Edgewise machine learning automatically derives actionable security policy from hundreds of thousands of interconnected network paths, and continuously refines these policies as the application landscape changes and evolves. This patented technology ensures your container infrastructure and the services it supports are always protected.

Detect potential attacks against applications in real time

Zero trust is at the core of Edgewise security policies. This means that every time an application attempts to communicate—from a container, to a container, or within a container—its identity must be cryptographically verified *before* a communication is sent and prior to its receipt by its target. Only Edgewise can assure symmetric authorization and authentication of application network flows inside containerized environments.

The same tools and technology that protect containerized workloads also detect anomalous behavior. Since security is tied directly to the identity of your communicating applications and services, if a fingerprint changes, security administrators are alerted in real time and can take immediate action without disrupting the development workflow.

Zero Trust Security For Any Container Environment

Edgewise's zero trust security platform provides the broadest coverage across all environments, whether it is bare metal on premises, virtualized private cloud, or the public cloud. Supported container environments include Kubernetes, Docker, and AWS Elastic Container Service (ECS). Edgewise's platform and products are API driven and can integrate with existing security tools and DevOps processes.

Why Edgewise

Increases developer speed

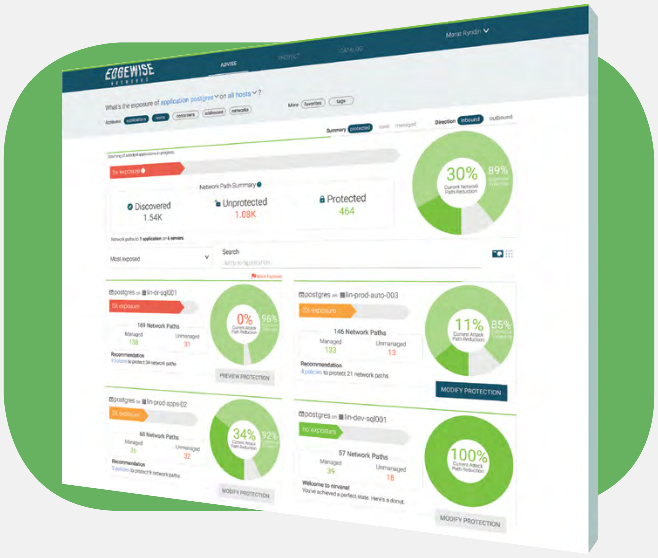
The automatically-created Edgewise policies are workload-centric and require no changes from development through production networks. Yes, Edgewise is CI/CD friendly.

Microsegmentation with one click

Edgewise abandons address- and network-reliant micro-segmentation approaches and instead builds policies that are based on software identity—simpler and stronger segmentation, with fewer policies to manage.

Zero trust security for container and non-container applications

Segment applications, hosts, and processes into "secure zones" within your cloud or data center



Welcome to nirvana!
You've achieved a perfect state. Here's a donut.

About Edgewise Networks, Inc.

Edgewise's Zero Trust Auto-Segmentation delivers impossibly simple microsegmentation in one click. Driven by machine learning, our patented Zero Trust Identity (ZTID) automatically builds cryptographic identities for all software and devices. ZTID bi-directionally verifies all software communications in your cloud and data center — every time workloads communicate. Reveal attack paths, protect applications, and measure security improvement. Gartner has recognized Edgewise as a 2018 Cool Vendor.

www.edgewise.net | @EdgewiseNet