EDGEWISE NETWORKS

DATA SHEET

Empowering DevOps With Zero Trust Security

Edgewise closes the security gap between the application and network.

Today's network security products rely on addresses, ports, and protocols, and inspecting network traffic. However, IP addresses don't create connections - software running on a server does. Edgewise closes the gap between the application and network with Zero Trust protection that verifies the identity of the software, users and hosts that are communicating. Edgewise's adaptive protection integrates with DevOps tooling.

Gain application and risk visibility

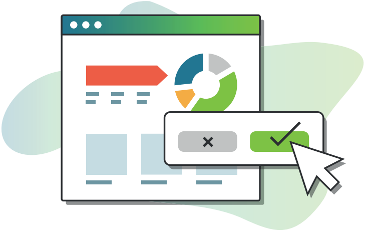
Edgewise analyzes and visualizes application topology and dependencies, provides recommended defensive measures, and quantifies the risk exposure and impact of applying controls. Operations teams can make more informed decisions around which controls to apply. DevOps and DevSecOps teams now have a collaborative understanding of the risk impact of security controls and how that evolves over time.

Define and maintain fine-grained access policies without introducing complexity

Edgewise "policy compression" methods use machine learning to automate definition of an optimal policy set using orders of magnitude fewer rules. This lets you define adaptive access controls that enforce "least privilege" without manually defining and maintaining thousands of policies.

Enforce access controls without impacting the application

Edgewise's Trusted Application Networking product protects business-critical infrastructure without changing the application or the network infrastructure that supports it. Edgewise requires no code changes, and introduces no VPNs, proxies or overlays, making deployment much simpler.



Integrate Zero Trust security into DevOps process tools

Edgewise's code-free integration with security and analytics tools gives DevSecOps and DevOps teams the context they need to validate Zero Trust controls, and recommend changes to developers with a single mouse click. Edgewise also incorporates a rich API set to automate and integrate policy creation and validation into the CI/CD pipeline.

Why Edgewise

Zero Trust allows only verified software to communicate.

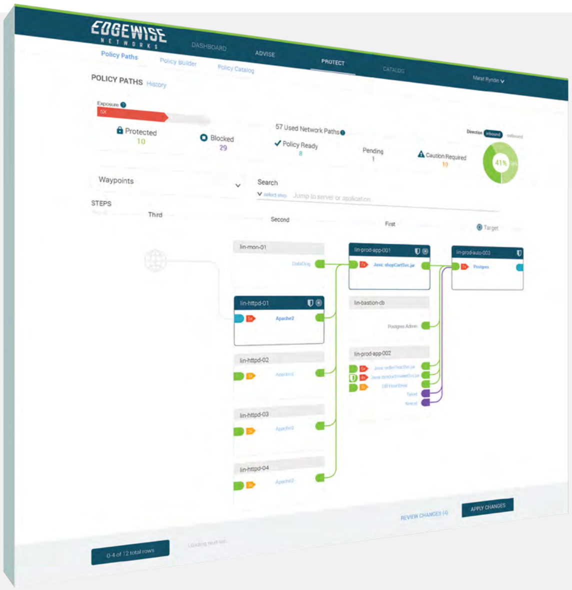
Secures production systems while enabling developer access.

No policy changes needed through the DevSecOps process.

Automatically builds policies within 72 hours.

Integrates with DevSecOps tooling.

Adapts to every cloud—VMware, AWS, Azure, and Google.



Edgewise **Protect**

Security operators need a new way to stop attack progression when legacy tools are no longer effective in the cloud. Edgewise Protect reimagines network security to protect where firewalls fail. Machine learning makes protection as easy as one click, while dramatically raising the cost and complexity for the attacker. **Request a demo**

Zero Trust Protection For Application Workloads

Stop lateral movement of malicious software in untrusted cloud networks by allowing only verified applications to communicate over approved pathways.

Eliminates Network Attack Surface

Over 95% of network pathways are not required for normal business use. Eliminate unnecessary attack surface and protect the rest with zero trust policies.

Faster DevOps Security With Automated Policies

Edgewise automatically builds protection policies using machine learning, within 48 hours. Simply click Approve for zero trust protection.

Azure Google Cloud Platform aws vmware® Windows

edgewise.net/demo

About Edgewise Networks, Inc.

Edgewise is the industry's first Zero Trust platform for hybrid cloud security. It stops attackers' lateral movements and protects workloads by allowing only verified applications, users, containers and hosts to communicate. Using machine learning, Edgewise recommends adaptive policies that eliminate 98% of the attack surface and protect the rest.

www.edgewise.net | @EdgewiseNet