EDGEWISE
ZERO TRUST NETWORKING

DATA SHEET

Edgewise for Increasing Business Speed and Agility

Today's businesses strive to operate at lightning speed, and address- and port-based security controls can be contrary to those initiatives. Whenever a port is blocked or a host is shut down because of a possible intrusion, employees are unable to access the data or services required to do their jobs. When a breach occurs, business disruptions accompany it. When the development team starts to deploy an application and security says, "No, stop. That's insecure," release is halted (and frustrations flare).

Operations and application/development/engineering teams often have differing perspectives from the security team, based on the fact that their initiatives and incentives are prioritized in sometimes-conflicting ways. The friction is compounded when security feels it is repeatedly excluded from decisions about what hardware, software, and applications are deployed.

Reduce friction between teams

Software and applications dominate business, and the formation of DevOps paved the pathway for today's rapid development. Unfortunately, security's goals and processes often run counter to those of DevOps teams, and traditional security tools are incompatible with modern infrastructure.

Edgewise solves the problem of conflicting goals and values by integrating security controls directly into the DevOps process. Edgewise's policies are application-based, meaning there is no need to interrupt development or release cycles to apply protection. In addition, because software identity is the basis for control decisions, development teams are free to update, patch, or otherwise evolve applications to suit business needs. This means that DevOps can build and deploy software as usual without worrying about security breaking applications or causing delays in production.

Apply fine-grained controls without adding complexity

To accomplish fine-grained control over and visibility into their networks, companies have traditionally implemented microsegmentation. However, one major problem with network-based microsegmentation is the abundance of policies required to ensure each "secure zone" on the network is, in fact, secure. Network and security teams end up writing and managing thousands of policies so valid traffic and systems can communicate securely, which generally results in either overly permissive policies or overly restrictive ones, both of which cause huge headaches.

Edgewise uses machine learning to automate zero trust policy creation, which results in orders of magnitude fewer rules while achieving the highest level of security and significantly simplifying network and security teams' abilities to manage the network. All policies enforce least-privilege access and are highly adaptive to network changes and application upgrades, without requiring code changes, adjustments to network configurations, or introducing VPNs, proxies, or overlays that make traditional deployments much harder.

Remove traditional security roadblocks

Change management of traditional network security controls is a slow and cumbersome process, often involving manual ticketing for mundane tasks such as the addition of a port on a firewall rule. Address-based controls hinder application agility and add complexity in private, enterprise-managed network segments, and this drag is compounded in public cloud environments where the network is highly dynamic.

With Edgewise, security policy is based on software identity rather than address-based attributes, so organizations can be certain protection is always applied directly to critical assets rather than just the network they're traversing. As a zero trust platform, only authorized and authenticated applications can communicate in the expected environment, with identified dependencies. Edgewise allows organizations to deploy policy once and segment topology once; no more late night firewall changes, change-control boards, or untested rollback plans.

About Edgewise Networks, Inc.

Edgewise is the industry's first zero trust platform that stops breaches in the data center and cloud. It protects workloads and prevents attackers' lateral movements by allowing only verified software to communicate. Using machine learning, Edgewise recommends adaptive policies that eliminate 98% of the network attack surface and protect the rest. Gartner has recognized Edgewise as a 2018 Cool Vendor.

www.edgewise.net | @EdgewiseNet