EDGEWISE NETWORKS

DATA SHEET

Edgewise for Risk Reduction

Many organizations struggle to know precisely what data they have, where the data reside, and how data travels throughout the network. With Edgewise, any applications or services which attempt to communicate inside the network are identified, fingerprinted based on cryptographic attributes, then checked for verifiable authentication and authorization. This process allows security, IT, and networking teams to understand which applications and services are communicating on the network and stop malicious software or services from communicating.

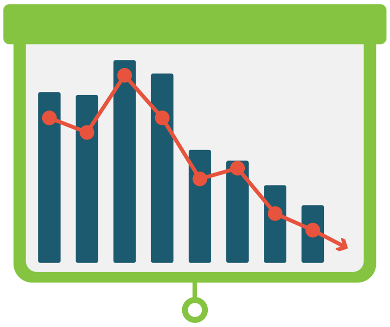
Improve visibility

From data to applications, hosts to users and devices, before the enterprise can manage the network, it's critical to build a current and accurate assessment of:

- What's present on the network
- What's communicating on the network
- How communications are happening
- Baseline normal activity

Gaining this type of visibility in an on-premises network is a big enough challenge. Now consider that organizations' networks are spread across multiple clouds and container environments, too.

With Edgewise, companies will always have an up-to-date communication map of all networked assets, which increases data awareness and affords the ability for a risk assessment of network overexposure. Every time workloads communicate through the network, Edgewise uses our fingerprinting technology to identify and reveal deeper insight about the current state of the network and provide recommendations for reducing network attack surface.



Quantify the state of your network

To truly quantify risk, organizations must know:

- Do we have a full view of everything on my network?
- How big is the network attack surface? Is it changing?
- How quickly can we identify vulnerabilities or attacks in progress?
- Can we remove outdated policies that slow down the network or prohibit innovation?

Companies' executive teams and boards of directors operate by constantly and continuously assessing right, and because cybersecurity has become a top-line business risk, they need quantifiable, point-in-time assessments for network risk.

Edgewise uses a zero trust methodology to identify applications and services that attempt to communicate, protect network assets with fine-grained software-based controls, and monitor the state of the network at all times. As a result, security, IT, and networking teams can understand, quantify, then communicate the risks associated with the network. Further, because Edgewise's risk assessments update in real time, organizations can measure progress against goals and demonstrate visible risk reduction. And what business leader doesn't want to see that?

Gain greater control

Security practitioners' greatest and longest-held fears of moving to and using public cloud are loss of visibility and lack of control. Despite the evolution in cloud service providers' security due diligence, security of what's *in* the cloud remains the responsibility of the cloud consumer — it's a shared responsibility model.

Edgewise is tailor-made for any type of network — including public cloud.

Our zero trust platform:

Restricts

Restricts communication by allowing only software verified by its identity to communicate.

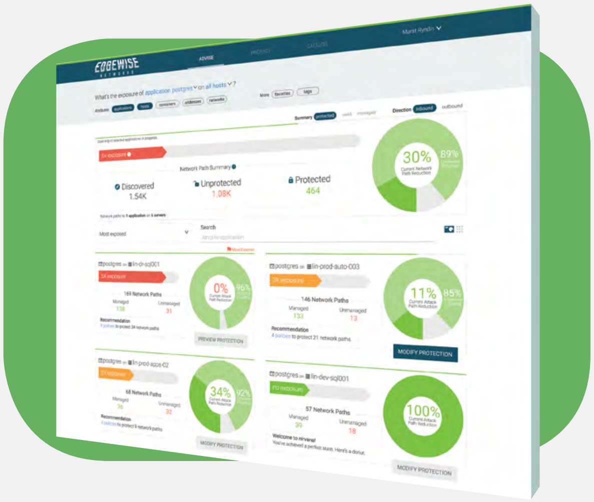
Eliminates

Eliminates unnecessary network attack surface in one click.

Automatically Detects

Automatically detects and adjusts to changes in the environment.

With Edgewise, companies gain uniform control over their network risk, which saves time and effort, and reduces friction with DevOps teams when new, business-critical applications are added to the environment.



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

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