EDGEWISE NETWORKS

DATA SHEET

Edgewise for Cloud Migration

Studies indicate that many organizations today maintain some level of on-premises data center use, yet most are steadily increasing their adoption of and investment in public, private, and multi-cloud networking environments. In fact, hybrid cloud is the most prevalent strategy among SMB and enterprise organizations[1] alike. This cloud-first movement is no surprise given that businesses have spent years advocating the financial, productivity, and accessibility benefits of cloud tools and technologies.

Protecting against data breach and unauthorized access are top concerns of IT and security professionals whose organizations are migrating to cloud services. This is no surprise; technology practitioners have grown used to a certain level of control over their internal networks and feel relatively confident in the protection mechanisms implemented on premises. When the network moves to someone else's infrastructure, however, that level of control is diminished and reliance on the provider is increased. But cloud security is a shared responsibility model. As the saying goes: Security *of* the cloud is the responsibility of the provider. Security *in* the cloud is the responsibility of the user.

Edgewise returns control to cloud consumers by providing stateless, adaptive security policies that are tied to your software and applications, not the environment in which they are communicating.

Edgewise allows companies to move to the cloud securely by placing protection at the application level instead of around every device, or end user. We help answer the questions: *Which applications are communicating? Which ones* should *be communicating? Are the right systems talking to one another without allowing malicious traffic to persist?* Built on zero trust, Edgewise allows only verified software to communicate in your public, private, or hybrid cloud environment, mitigating risk, and offering the highest level of data breach protection. We accomplish this in three ways

1. Attack Surface Analysis

Edgewise automatically analyzes all possible network paths, identifies which ones are required by the business, and gives you the ability to eliminate unused attack surface in one click.

2. Workload Protection

Based on a zero trust methodology, Edgewise allows only verified software and hosts to communicate by automatically building and recommending segmentation policies that are rooted in the secure identities of communicating software.

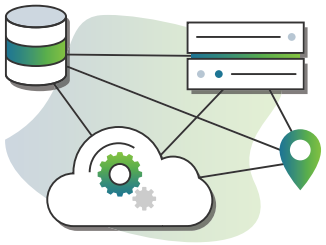
3. Application Monitoring

Edgewise provides greater accuracy than address-based monitoring tools which are location dependent. We use machine learning to baseline normal activity and alert you to potential attackers' lateral movements.

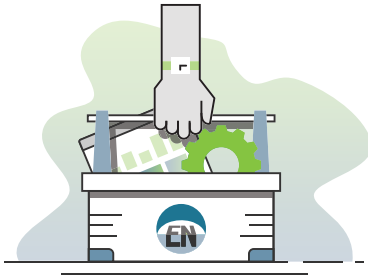
[1] https://www.edgewise.net/blog/network-security-findings-from-the-black-hat-business-hall

Edgewise helps your business:

Save time



Edgewise gives you the intelligence to understand and react to to risks on your network, without the heavy lift of writing and continually tuning security policies. We automatically map your application topology, visualize all potential attack pathways, and highlight areas of greatest risk, whether your workloads are running in the cloud or in an internal data center. Based on this data flow mapping, Edgewise automatically builds and recommends portable policies using machine learning, and all policies can be implemented in one click. Because Edgewise works across network environments, you no longer need to waste time creating and implementing different policies for different environments (public, private, or hybrid cloud). Edgewise protection travels with your workload, saving you time and increasing security.



Reduce complexity

In a service-oriented architecture, tracking inventory of policies and applied rules is difficult, and dependencies are affected every time a cloud instance changes. This creates management and availability issues. Additionally, data flow mapping in a cloud is complex because services can change location, which increases the number of data points that must be monitored and managed. In contrast, Edgewise simplifies tracking and protection and anticipates the impact of change by focusing on the data and applications rather than the environment in which they are running. Full integration with your CI/CD pipeline means that software is protected before it's deployed into your production environment. No more operational complexity of trying to determine which applications are talking to which servers, learn where each host is located, or monitor thousands of data points. All that matters is your data, and Edgewise applies zero trust protection at the software/application level, reducing the headache of managing ever-changing environments.

Apply gap-free protection

Cloud architectures are not fit for traditional security tools that are based on IP addresses, ports, and protocols. The dynamic nature of the cloud makes these static security controls unreliable because they can change at any time, multiple times throughout any given day. To counter the problem of address-based controls, Edgewise cryptographically fingerprints workloads based on a set of immutable properties that attackers can't exploit. Our zero trust, data-centric policies provide consistent, application fingerprint-level protection for your workloads, whether you start in the cloud or are migrating there, and do not require any changes after migration. You configure what you want to monitor and protect, and we will alert you any time your environment deviates from its expected state. Edgewise's uniform approach to policy creation and application means that you can be certain only software verified by its fingerprint is allowed to communicate—independent of network location.

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