EDGEWISE NETWORKS

DATA SHEET

Edgewise for Zero Trust Segmentation in Your Cloud and Data Center

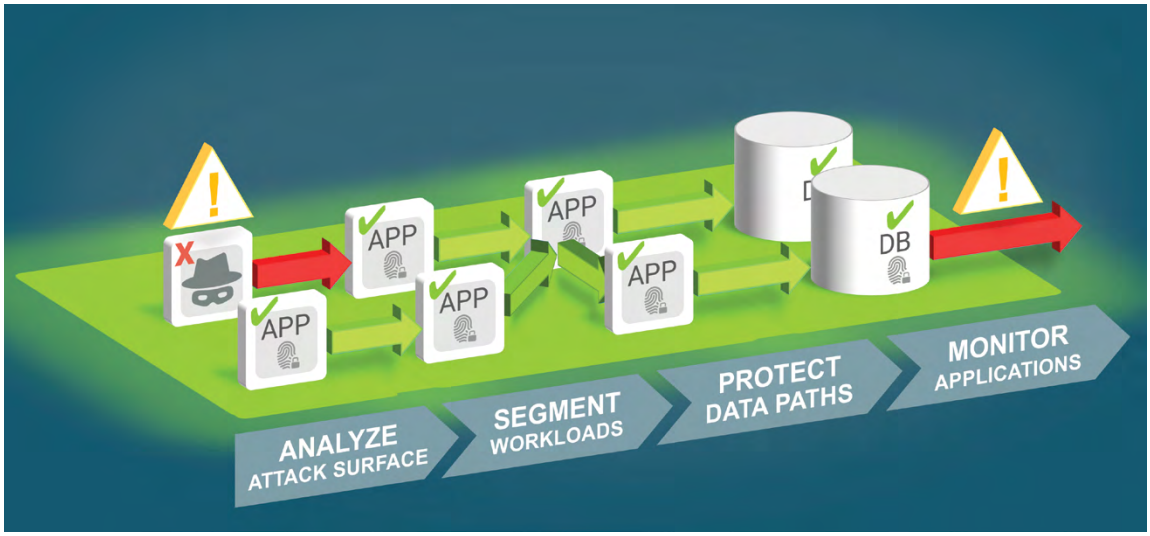
The attack landscape has evolved and today's threat actors target data-rich applications and services. However, most organizations have not evolved how they protect these business-critical resources. As a result, attacks keep occuring, the amount of data lost or stolen per breach keep rising, and the costs for dealing with the myriad aftereffects of an intrusion keep mounting. These problems persist because most of the communication pathways used in attacks remain undetected for long periods since traditional controls are ineffective at identifying when an adversary is hiding in "trusted" HTTPS traffic or when malicious software is piggybacking on address-based protocols, moving laterally inside the network to gain unauthorized access to systems and data.

Despite the risks, organizations continue to manage their networks using "trust zones"; anything inside a network perimeter is trusted after it passes through a security "checkpoint" and is therefore allowed to communicate freely. However, security practitioners have seen how attackers exploit trust and know that a new approach to network security is required.

Zero trust networking assumes that the network is hostile and treats all traffic—including traffic inside the perimeter—as untrusted. Before being allowed to communicate, every application, host, and process must be verified based on the identity of the software itself. Zero trust is data centric, creating microperimeters around your "crown jewels," and applies least-privilege access so that you immediately see a reduction in your network attack surface.

The Edgewise Advantage

Edgewise is the only zero trust platform that microsegments data and applications using the cryptographic identity fingerprint rather than address-based controls. We focus on the data first because that's what your adversaries are after. Further, Edgewise eschews the idea that address-based controls are adequate to protect your assets, especially in cloud environments where security teams have less control over the network. Edgewise supports all major cloud platforms.



Edgewise helps your business:

Support business initiatives, without traditional security roadblocks

Today's businesses need to be able to operate at lightning speed and utilize the tools and technologies that make employees optimally efficient and productive. Any threat to the confidentiality, integrity, or availability of data or systems is a priority business risk that must be mitigated.

Traditional security tools can be antithetical to speed and efficiency, but Edgewise offers a different approach. Edgewise places protection as close to your data as is possible. Our application-aware policies travel with all applications and services, meaning that potential compromises will be contained to the affected asset, not the entire network. In addition, with Edgewise, security teams no longer need to worry about shadow IT entering the environment. Edgewise automatically identifies all communicating software and recommends zero trust policies which can be applied with one click. Edgewise allows businesses to operate most effectively while providing the highest level of security control possible.

Apply gap-free protection

Security tools that rely on IP addresses, ports, and protocols are not fit to protect cloud architectures. 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. Even in an on-premises environment, organizations need to recognize that today's attackers can easily piggyback on or spoof traditional network security controls, making them less effective for breach protection.

To counter the problem of address-based controls, Edgewise cryptographically fingerprints workloads based on a set of immutable attributes that are used to provide consistent protection for your workloads, whether you're operating in an internal data center or the cloud or are migrating to the cloud. This approach decouples your workload security from IP address constructs and therefore allows you to avoid issues with IP-based controls. Edgewise's uniform approach to policy creation and application identification means that you can be certain only software verified by its fingerprint is allowed to communicate—independent of network location.

Continually assess risk

Most security practitioners know that their corporate networks are vulnerable to compromise, but most can't quantify the level of risk these networks pose to the organization, particularly related to application exposure. Edgewise automatically measures your visible network attack surface to understand how many possible application communication pathways are in use, quantifies risk exposure, and uses machine learning to recommend zero trust security policies that dramatically reduce your probability of data breach.

Based on the principle of least-privilege access, zero trust networking reduces the access applications, hosts, and processes are granted inside your network. But Edgewise takes it one step further by verifying the secure identities of communicating software every time software requests a communication. Our software-centric approach mitigates risk and provides visualized risk reports that allow you to easily filter by applications or hosts.

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