EDGEWISE NETWORKS

DATA SHEET

Edgewise for Mitigating Breach Potential

Edgewise is focused on the software and services communicating in your network so it's easier for security and operations teams to quickly identify and stop malicious activity. Edgewise continuously inspects connection requests for deviations from the intended state and prevents unverified assets from communicating anywhere on the system. Any altered application or service, whether it's a result of adversarial activity, misuse, or accident, is automatically untrusted until it can be re-authorized and authenticated. Further, even when verified and approved, communication is restricted to least-privilege access, resulting in decreased attack surface.

Lower risk

Organizations run on network-connected software, data, and services.
The gains in productivity and ease of use cannot be ignored, but with every network interaction comes a hightening degree of risk. Businesses rely on network and security teams to ensure uptime and availability while maintaining the privacy and security of networked assets. Additionally, business executives expect IT teams to communicate the realistic risk of data breach or compromise so market, financial, and product decisions can be made.

Protect your assets

In a modern-day threat environment of, "It's not 'if' but 'when,'" organizations need to be very strategic about how they protect their networks and the applications and services that communicate inside them. Protecting networks is hard enough when systems reside on-premises, but most companies have the added of challenge of applying security control to hybrid cloud environments where network constructs change frequently.

Traditional address-based tools are ineffective in highly-dynamic environments, so Edgewise use a software-centric approach. By cryptographically fingerprinting all software and services, then applying zero trust principles which ensure every communication is verified before it's allowed to send or receive, Edgewise provides gap-free protection, independent of network location.

Continuously monitor and assess

The Edgewise zero trust platform is focused on the workload so it's easier for security and operations teams to identify and stop malicious activity. Edgewise continuously inspects workloads for deviations from the intended state and prevents those which are unverified from communicating anywhere on the system—to and from command and control, and between hosts, users, or applications. Any altered application or service, whether it's a result of adversarial activity, misuse, or accident, is automatically untrusted until it can be verified again through a set of policies and controls. Additionally, even when verified and approved, communication is restricted to a "need-to-know" basis, i.e., access is locked down to only the users, hosts, or services that fundamentally require access.

This inherent distrust results in decreased breach potential and therefore decreased risk, not to mention lower costs for cleanup and mitigation (since there are fewer breaches to handle).

Edgewise helps network, operations, and security teams assess and express risk in three ways:

Visualize

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut la adipiscing elit, sed do.

Protect

Protect networks with zero trust, software-centric security controls which cannot be separated from the assets business need to protect most.

Monitor

Monitor what's present on the network, what's communicating on the network, how communications are happening, and baseline activity to quickly identify when deviations from expected state occur.

See how Edgewise makes zero trust segmentation simple for defenders and complex for attackers.

REQUEST DEMO

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