EDGEWISE
ZERO TRUST SEGMENTATION

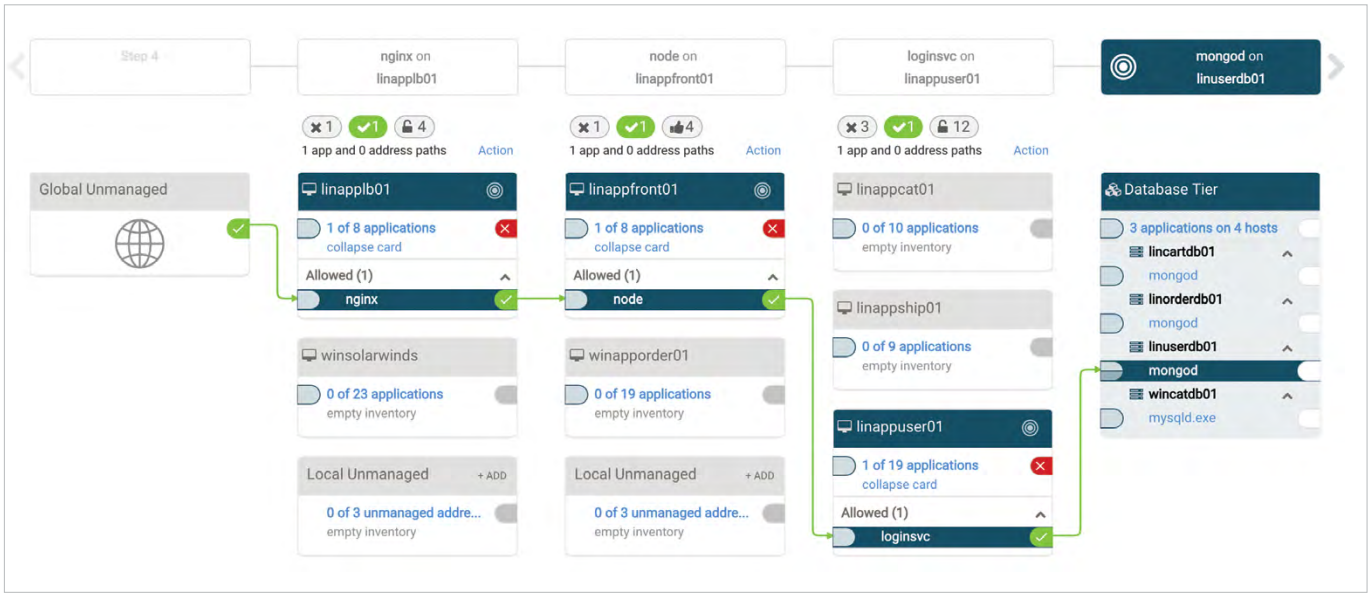
SOLUTION BRIEF

Zero Trust for Cloud Workload Protection

The vast majority of enterprises have adopted a cloud strategy. To meet market demand and ensure customer satisfaction, the major cloud providers like AWS, Azure, and Google are improving their cloud-native infrastructure security and promoting it as a competitive advantage. However, under the Shared Responsibility Model, cloud consumers retain responsibility for what's communicating in the cloud, in other words, their data.

The ephemeral nature of the cloud is an attacker's paradise. Legacy security tooling works on a trust model that is no longer valid in today's threat landscape. Perimeters have all but disappeared, encryption makes traffic inspection difficult, and classifying distributed data is resource intensive. All of this means that even if traffic were to pass through a north-south perimeter gateway, identifying and stopping "bad" would be challenging. However, most traffic in a cloud environment is east-west, where traditional security controls do not apply.

Legacy network-based technologies don't translate well into cloud environments which are elastic, loosely coupled to infrastructure, and do not have a static perimeter at which to place security controls. Stronger, provable cloud workload protection today depends on companies' abilities to put applications and services, themselves, at the center of the protection plan. The new imperative is to move access controls away from the network paths applications traverse and tie them directly to the identity of communicating applications and services. It's no longer sufficient to define software by its traffic route. Security control must be workload-centric and not coupled with the cloud platform, because workloads in cloud provider environments are not.

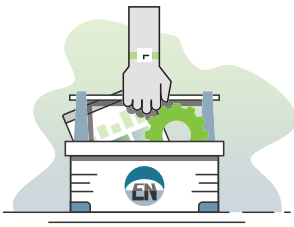


Edgewise Data Mapping Dashboard.

The Edgewise Advantage

Edgewise allows companies to protect cloud workloads 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 workloads to communicate in your public, private, or hybrid cloud environment, mitigating risk, and offering the highest level of data breach protection.

Edgewise helps your business:



Reduce complexity

In a service-oriented architecture, tracking asset and policy inventories 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 applications rather than the environment in which they are communicating. 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 level, reducing the headache of managing ever-changing environments.

Apply gap-free protection

Cloud architectures are not fit for traditional security tools that use IP addresses, ports, and protocols as the control plane. 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 software based on immutable properties that attackers can't exploit. Our zero trust, identity-centric policies provide consistent workload protection and do not require any cumbersome architectural changes. Apply recommended application segmentation policies in one click, and all of your cloud-based workloads are protected uniformly and 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 based on the criticality of communicating software, and uses patented machine learning to recommend the fewest number of zero trust security policies that dramatically reduce your probability of data breach while remaining easy to manage.

About Edgewise Networks, Inc.

Edgewise's Zero Trust Auto-Segmentation delivers impossibly simple microsegmentation in one click. Driven by machine learning, our patented Zero Trust Identity (ZTID) automatically builds cryptographic identities for all software and devices. ZTID bi-directionally verifies all software communications in your cloud and data center — every time workloads communicate. Reveal attack paths, protect applications, and measure security improvement. Gartner has recognized Edgewise as a 2018 Cool Vendor.

www.edgewise.net | @EdgewiseNet