EDGEWISE
ZERO TRUST SEGMENTATION

DATA SHEET

1-Click Zero Trust

Auto-Segmentation For Hybrid Cloud

Microsegmentation that's impossibly simple

Cyber threats need attack paths to reach vulnerable targets. The most effective way to reduce the network attack surface is segmentation. Experts agree that microsegmentation is a core protection strategy for workloads, however, the time required, complexity, and cost of implementing segmentation has historically outweighed the security benefit.

Not anymore.

Edgewise is a new way to microsegment your environment. It's impossibly simple and all it takes is one click. Reduce risk and erase operational effort by allowing Edgewise to reveal risk and apply identity-based protection to your workloads, without any architectural changes to your networks, and no reboots. Edgewise's software identity-based model provides gap-free protection with policies that automatically adapt to the environment in which they're running. Eliminating your network attack surface has never been simpler.

The Benefits of Application-Aware Control

Cloud and data center networks are full of data that's attractive to cyber criminals. Despite the strength of your perimeter controls, cyber criminals can access your network through phishing or some other form of social engineering. With a traditional network-based security strategy, once an attacker has stolen credentials or exploited a vulnerability to gain access to the network, they can "feed off the land" — introduce malware and move laterally inside trusted network communication paths to gain unauthorized access to critical applications. Network compromise can be highly disruptive, causing far-reaching financial, reputational, and operational damage. To prevent unauthorized east-west communications, organizations need security controls to center on the *verified identity of approved applications*.

Edgewise allows businesses to become application aware and to protect any network from application compromise with zero trust security controls based on the cryptographic identity of communicating software.

Edgewise Value

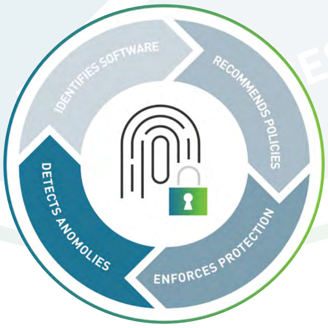
Provides full visibility into east-west network communications

Patented identity-based policies that adapt to your dynamic environment

Agent-based protection for maximum security and performance

Effortlessly optimizes policies for **risk reduction** and **operational ease**

Provable return on your security investment



Embrace A Zero Trust Approach

Edgewise's zero trust, workload identity-based approach abandons the traditional security model of allowing application communication based on trusted IP addresses, ports, and protocols. Our zero trust model treats internal communications like the internet: potentially hostile and filled with threats. Only applications and services verified by their cryptographic identity are allowed to send and receive communication—resulting in stronger security that works wherever your applications do.

Patented Identity-Based Auto-Segmentation

Legacy microsegmentation involves multiple steps that can take months. Edgewise microsegmentation happens in mere minutes—with just one click. From asset inventory to mapping data flows to deploying policies for enforcement, our microsegmentation is quick and simple.

Edgewise protects critical data and applications in the hybrid cloud through a fundamentally new control plane: software identity. All software in an Edgewise-managed environment is fingerprinted using a combination of cryptographic identity attributes. Software identity is the basis for every access control decision. Per our zero trust model, if software can't be verified, it can't communicate, regardless of previous permissions. This ensures the strongest level of protection for your workloads, independent of network changes.

This new methodology means that security control adapts to any environment—with fewer policies to manage. Edgewise zero trust auto-segmentation provides stronger, simpler, scalable protection for hybrid clouds with six differentiating attributes:

Policies built automatically

Risk is reduced through policy compression

Security outcomes are provable

Software identity verified through cryptographic attributes

Segments adapt to accommodate application updates and changes

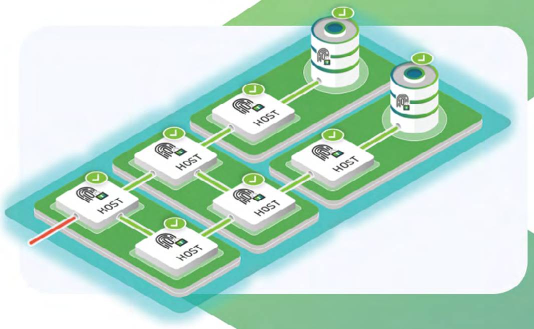
Security monitoring tools are enriched with app data

Zero Trust Identity

The technology that drives Edgewise's automated microsegmentation is based on zero trust identity (ZTID). Identity attributes that comprise a workload's identity include the SHA256 hash, fuzzy hash, executable signing, PE header values, UID, CPU serial numbers, provisioned host name, and more. Each unique identity informs the machine learning that builds recommended policies and is used for access control decisions. Because Edgewise policies are zero trust, only software that can be verified by its ZTID is allowed to communicate on your networks, creating a more secure yet operationally efficient network.

Simpler for operations

Instantly microsegment your environment—with one click. Your business applications are automatically protected and operational. No network changes required. No need to manually build or update a single policy. And lengthy deployment schedules are history.

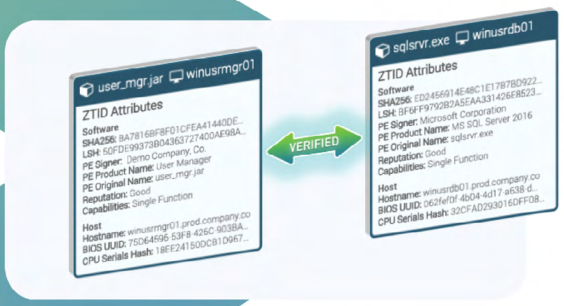


Stronger for security

Define microsegmentation boundaries based on interdependencies of communicating software—not IP address. Prevent malware propagation and abuse of admin tools by verifying software identity to authorize communications in your cloud and data center, and ensure that only valid business applications communicate.

Scalable for DevOps

As your workloads are deployed, guarantee they always have the required access for smooth business operations. As your environment auto-scales, Edgewise policies adapt automatically across VMs and Kubernetes containers, on premises, or in the public cloud.



user_mgr.jar winusrmgr01

ZTID Attributes

Software
SHA256: BA7816BF8F01CFEA41440DE...
LSH: 50FDE99373B04363727400AE98A...
PE Signer: Demo Company, Co.
PE Product Name: User Manager
PE Original Name: user_mgr.jar
Reputation: Good
Capabilities: Single Function

Host
Hostname: winusrmgr01.prod.company.co
BIOS UUID: 75D64596-53F8-426C-903BA...
CPU Serials Hash: 18EE24150DCB1D967...

sqlsrvr.exe winusrdb01

ZTID Attributes

Software
SHA256: ED2456914E48C1E17B7BD922...
LSH: BF6FF9792B2A5EAA331426E8523...
PE Signer: Microsoft Corporation
PE Product Name: MS SQL Server 2016
PE Original Name: sqlsrvr.exe
Reputation: Good
Capabilities: Single Function

Host
Hostname: winusrdb01.prod.company.co
BIOS UUID: 062fef0f-4b04-4d17-a638-d...
CPU Serials Hash: 32CFAD293016DFF08...

Centralized Management for Your Multi-Cloud, Hybrid Cloud Environments

Edgewise provides the broadest support across all environments, whether it is bare metal on premises, virtualized private cloud, the public cloud, or any combination thereof. Environments can be static or highly dynamic. Edgewise supports 10 distributions of Linux (with over 800 patch levels dating back to 2.6), Windows 7 onwards, and any Windows Server operating systems. Supported container environments supported include Kubernetes, Docker, and AWS Elastic Container Service (ECS).

Edgewise's continuously adaptive platform and products are API driven. Edgewise can integrate with existing security tools and DevOps processes, enabling 1-click auto-segmentation.

Linux Windows Windows Server kubernetes docker Amazon ECS

Azure Google Cloud Platform aws vmware

Edgewise Zero Trust Segmentation Use Cases

Zero trust for cloud workload protection

Protect your business-critical applications across cloud environments from one central platform.

Data flow mapping for visibility

Visualize your application topology and see when changes occur.

Event correlation and security monitoring

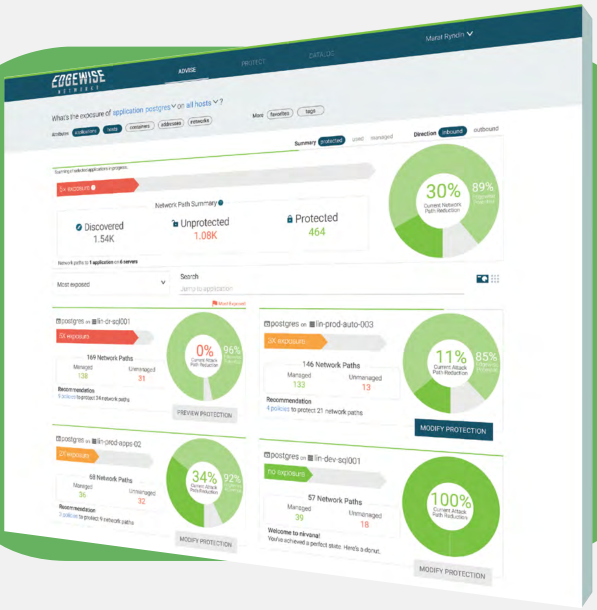
Feed your application communication logs directly into your SIEM, enabling remediation prioritization.

Zero trust microsegmentation for compliance

Segment applications into “secure zones” to see and stop compliance violations before they happen.

Container security

Protect applications in ephemeral production environments without disrupting the CI/CD workflow.



What's the exposure of application postgres on all hosts ?

Scanning of selected applications in progress.

Network paths to 1 application on 6 servers

Recommendation
9 policies to protect 34 network paths

Recommendation
4 policies to protect 21 network paths

Recommendation
3 policies to protect 9 network paths

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

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.

Gartner
Cool Vendor
2018

www.edgewise.net | @EdgewiseNet