EDGEWISE
ZERO TRUST SEGMENTATION

SOLUTION BRIEF

Edgewise for Event Correlation and Unified Security Monitoring

SecOps teams are bombarded with information about the network. Digital transformation offers myriad organizational benefits, but the requirement to constantly monitor the security and health of every system on the network is a massive operational burden. To ensure the confidentiality, integrity, and availability of all systems and their data, operations teams must analyze mountains of logs and scrutinize dashboards continuously. Monitoring responsibilities are further challenged by the fact that most organizations' technology implementations have grown piecemeal, adding relevant hardware and software as needed and as it becomes commercially available from standalone, best-of-breed solution providers. This "bolting on" of technology is no more prevalent than in security, and has meant that operators and administrators must familiarize themselves with each tool's unique outputs in addition to correlating events across dissimilar platforms.

For these reasons, organizations have sought technology integrations that offer the proverbial "single pane of glass," in other words, technology that can correlate logs and data across platforms and present it in a way which facilitates rapid anomaly detection and threat mitigation.

The Edgewise Advantage

Edgewise allows companies to feed application communication logs from the Edgewise platform directly into their Security Information and Event Management (SIEM) platform. Free from the historical configuration, customization, and deployment complexity of traditional solutions, Edgewise integrates through a lightweight API which allows you to prioritize security events better, detect anomalous communication faster, and reduce alert fatigue. Our SIEM-ple API results in enriched SIEM data that accounts for the state of your business-critical applications and services.

Edgewise helps your business:

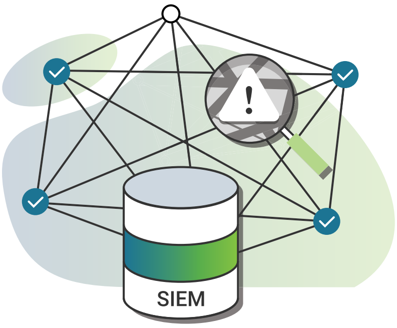
Achieve real-time threat visibility

Your Edgewise deployment provides insight and context for application communication in your cloud, on-premises data center, container, or virtual environment. The Edgewise Console gives you real-time visibility into application communication patterns and trends and alerts you when anomalous activity occurs. However, we know that logging into and monitoring disparate consoles can be cumbersome; the more places you have to audit for threat activity, the more likely you are to miss critical alerts.

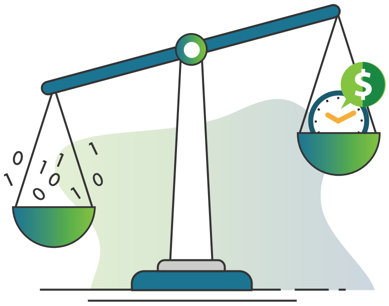
Using machine learning, Edgewise builds application-centric segmentation policies that are decoupled from the network, meaning that you always have an up-to-date picture of what's happening on your networks. Feeding your Edgewise application data directly into your SIEM allows for greater coordination and contextualization across all sources of network activity. The result? More accurate detection at a faster pace through one, centralized location.

Improve network security and compliance initiatives

The SIEM is an invaluable tool to track network operations, detect potential issues against the infrastructure, and investigate unusual activity. The coordination of log data from various sources helps companies quickly identify security events and compliance violations. But as the saying goes, "garbage in, garbage out." Without the right data, it's impossible to generate reports with sufficient detail about security events.



Your Edgewise SIEM-ple integration ensures that your SIEM tool of choice receives accurate, real-time information about the state of your applications, across any network environment, independent of network constructs. Our zero trust, identity-based microsegmentation guarantees that you are feeding your SIEM the right data, allowing you to make better, faster cybersecurity decisions and prove compliance requirements are always met.



Decrease operational costs: Saves time and money

A primary use case for SIEM is the ability to correlate workflow processes and associated log data across an organization's infrastructure. SecOps teams gain a unified view of network activity, which means less time and effort to prioritize, triage, and respond to alerts.

The information you send to your SIEM through your Edgewise integration reduces operational costs more than traditional microsegmentation tools because our zero trust segmentation policies are based on the cryptographic identity of your communicating applications and are independent of network constructs. How does this help with operational cost reduction? Today's networks are noisy and complex, and traditional tools that rely on IP addresses, ports, and protocols are unreliable in ephemeral environments like cloud and containers. Edgewise, in contrast, simplifies microsegmentation through zero trust and machine learning, resulting in 25x fewer policies to manage and information about your network attack surface that's 100% reliable. The network analysis from Edgewise's solution is data-specific and inextricably linked to your applications—the data-rich sources targeted by cyber criminals. As such, your SIEM receives the best data about the security of your applications, which results in immediate, provable security outcomes.

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