EDGEWISE NETWORKS

DATA SHEET

Edgewise for Segmenting Compliance Environments

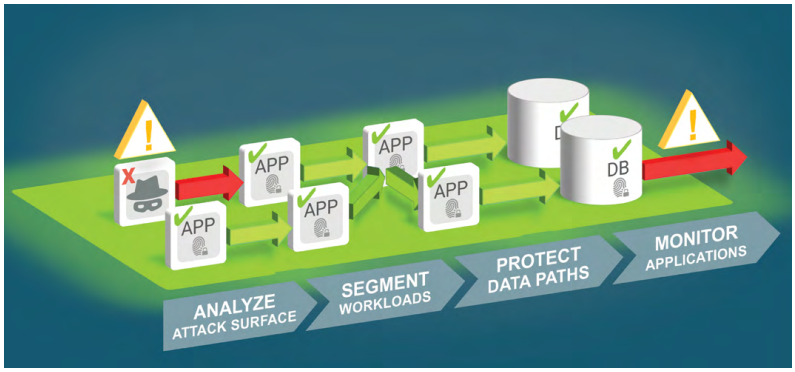
Compliance is a functional area that weighs heavily on security practitioners' minds. Though "compliance doesn't equal security," all security practitioners understand that meeting compliance requirements is an important business initiative and therefore one that cannot be ignored. Compliance, too, has been a driver for attaining cybersecurity budget, which makes it a reliable lever for security teams to push when looking to increase resources. Therefore, while security practitioners may have mixed feelings on compliance, the bottom line is: While compliance does not equal security, compliance—when done correctly—can be the foundation of a thorough and effective cybersecurity program, a foundation upon which security and IT teams can build hardened environments for their organizations' data and systems.

More than 25,000 new cybersecurity and privacy regulations have been introduced since 2008, resulting in increased responsibility for security teams. It is incumbent upon security teams to find and protect all data and systems in scope for relevant compliance mandates. From PCI-DSS to HIPAA to FISMA to Sarbanes Oxley, security teams must keep abreast of individual guidance and requirements and determine the best strategies which allow them to demonstrate compliance.

Edgewise Advantage

Edgewise is a zero trust software-based solution that segments applications, hosts, and processes into "secure zones" within your cloud, onsite data center, or hybrid environment. With Edgewise, organizations can identify compliance-related data communicating in their networks, segment that data away from other, non-scope data, then build and recommend appropriate security policies to keep the data secure and private.

To illustrate, the PCI Security Standards Council specifies that all systems located within and connected to a credit card data environment are in scope for the PCI-DSS. Further, "in a flat network, all systems are in scope if any single system stores, processes, or transmits account data."[1] Network segmentation eliminates the problem of flat networks and prevents lateral movement. Edgewise not only segments each workload in your cloud or data center, but does so by implementing a zero trust framework, which means that every time an application, host, or user account requests a communication, it must meet verification requirements before communication is allowed. And unlike address-based segmentation technologies, Edgewise uses the cryptographic fingerprint of the workload to verify the validity of a workload so that your protection is viable in highly dynamic, auto-scaling environments. Edgewise's zero trust segmentation gives security teams assurance that wherever data and systems in scope for compliance reside, it is covered by reliable security controls that can't be separated from the workloads themselves.



[1] https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

Edgewise helps your business:

Gain visibility and map data flows

A critical element of assuring your data and systems can meet compliance requirements is first gaining an understanding of how data is stored and transmitted through your network environments.

Edgewise maps your application topology and provides complete visibility into network communications by fingerprinting all software and services based on identity attributes like the SHA256 hash, file path, and loaded modules.

Every time workloads communicate through the network, Edgewise is able to accurately determine what's communicating and reveals deeper insight about application-to-application communication, connections between hosts, and other data pathways.

To learn whether systems are compliant to any given regulation, you need visibility into data flow. Edgewise provides network visibility and simplifies data mapping by focusing on the data and applications that are communicating rather than guessing about the state of your network based on application protocols.

Identify violations

When managing compliance, security and audit teams must be able to identify how data is being accessed and by what services or processes.

Because Edgewise fingerprints then segments every host and application communicating in your networks, and then uses zero trust verification to approve or deny network communications, you can instantly identify violations of privacy or security laws (e.g., transferring or storing health data to a non-compliant database) and the potential for privacy abuses (e.g., if a database containing PII tries to connect to an unverified host).

Edgewise allows you to block risky network communications with one click.

Secure data according to its sensitivity

Segmenting your network reduces the scope of compliance initiatives for your organization because different regulations put certain (and sometimes disparate) types of data in scope. In a zero trust network, "microperimeters" are created for specific data types, assets, services, and applications.

Edgewise places these "microperimeters" at the data level instead of at the edge of the network, on users, or on user devices. Because Edgewise's segmentation policies are focused at the data level, they are better able to protect against malware propagation than perimeter-based or address-based controls, which may not be reliable in a cloud or container environment and can be easily spoofed by threat actors.

Edgewise's "data-first" approach means that you can apply policy based on data type and know that control travels with the data, independent of network environment. When it comes time for a compliance audit, your customized dashboard allows you to quickly and clearly demonstrate how compliance-related data and systems have been protected against unauthorized access or use.

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