EDGEWISE NETWORKS

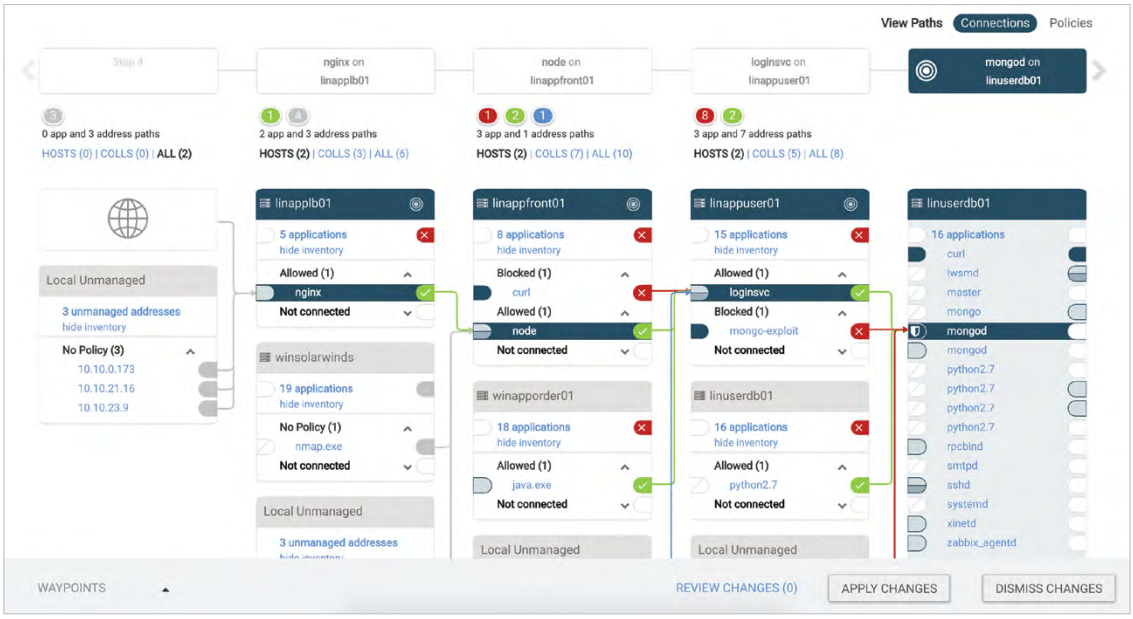
DATA SHEET

Edgewise for Data Flow Mapping

The Center for Internet Security (CIS) Controls are a well-known resource within the cybersecurity community, so it would be safe to assume that most security practitioners have some cognition that "inventory and control of hardware assets" and "inventory and control of software assets" are the #1 and #2 recommendations for protecting organizations and their data from cyber attacks. If these two actions are not yet on your cybersecurity roadmap, the Verizon Data Breach Investigations Report (DBIR) provides the reason why they should be: According to the 2018 DBIR, the #1 asset involved in data breaches is databases. Databases, of course, contain the sensitive data upon which businesses depend, and a breach of this data could be financially and reputationally catastrophic to your organization.

Today's businesses operate on increasingly distributed network architectures, which means critical data can be disseminated across numerous networked assets. Your software and applications contain data, your web and email servers handle data, and your data is constantly being spun up into cloud and other virtual instances where the security of the infrastructure is outside of the enterprise security team's control. To protect your data and the systems that contain the data, you need to understand:

- What data you have
- What data is communicating on your network(s)
- The sensitivity of that data
- How and when data is communicating
- Environmental risk due to overexposure of data pathways within the network



Edgewise Data Mapping Dashboard.

The Edgewise Advantage

The Edgewise zero trust platform allows network administrators and security teams to map data flows in any network environment, visualize which applications and hosts are talking to each other, and see when changes occur. Because Edgewise is application-aware, all network communication pathways in use are identified automatically and associated to the software sending and/or receiving the packets. In contrast, address-based technologies can see network traffic and identify the application protocol used, but can't see what, specifically, is communicating, and can't recognize when a malicious adversary has hijacked a network communication or if malware has been added to the environment. Since you cannot manage what you cannot see, a lack of application-aware capability means you are blind to risk. Edgewise gives organizations the ability to truly understand what's happening on their networks.

Edgewise helps your business:

Gain visibility

A critical element of protecting your networks, whether they are internally managed or managed by a cloud service provider, is first gaining an understanding of what is present and communicating on your network.

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 protect your key data assets, you need visibility into data flow. Edgewise 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.

Improve security auditing

A key operational security concern for security professionals is the ability to audit systems[1] for vulnerabilities and deviations from expected state.

Edgewise builds a zero trust-based, real-time, always up-to-date map of data flow so that you can clearly see how your software is communicating through systems; what applications, hosts, and processes have access to and are talking to other applications, hosts, and processes; and who/what is attempting third-party access. This insight is an important part of ensuring your systems have the proper controls implemented, that the controls are functioning as intended, and that systems are free of vulnerabilities or exploit.

By maintaining real-time, current information on workload communications, Edgewise gives you the confidence to exceed security and compliance audit requirements by implementing a zero trust networking approach.

Adapt to real-time changes

To be able to thoroughly protect your applications and software, it is vital to gain real-time visibility into workload communication patterns. Edgewise uses machine learning to learn your application topology, visualize all the potential pathways of attack, and highlight areas of greatest risk.

Because Edgewise is application-aware and not bound by network address constructs, you can be certain that active changes will always be recognized, independent of changes to environment such as new or retired instances in a cloud or container.

Your data map will automatically adapt, giving you an advantage over attackers by preventing any unverified workloads from communicating (i.e., implementing zero trust), whether your networking is happening in a cloud, onsite data center, virtualized environment, or any hybrid combination.

[1] https://www.edgewise.net/blog/network-security-findings-from-the-black-hat-business-hall

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