Why Perimeter Security Doesn't Work for the Cloud

For the past 40 years or so, and more recently with the use of next-gen firewalls and secure web gateways, there has always been an outwards vantage point for security. The reactive processes and technologies have revolved around deterring bad actors from infiltrating organizations, data and applications. Perimeter-based security intrinsically trusts everyone inside, affirming that if an address originates from a “trusted” virtual private cloud or network segment, the communication and actions were free of malicious intent.

As traditional constructs of on-site employees and on-premises solutions fade, and critical applications and data are moved to the cloud, security teams are left to question the effectiveness of perimeter security. The former sense of trust and control is evaporating, as policies are unable to keep pace with dynamic, scalable and distributed multi-cloud environments.

How Perimeter Security Fails Today

The complexity of today’s business ecosystems has driven industry experts like research and analysis firm, Forrester, to insist that the corporate perimeter is obsolete, and even dangerous. A recent report recommends organizations use a digital transformation mandate as a means to escape legacy networks full of “security debt.” Instead of bolting on security to fill the holes that perimeter security measures fail to protect, enterprises have the opportunity to build in entirely new methods and rethink their approach:

1. **Heterogeneous Environments Have More Work and Less Security**

   Many organizations work within a hybrid cloud environment, maintaining on-premises solutions in tandem with cloud-based resources and workloads. The problem with securing bifurcated architectures lies in the fact that modern cloud workloads are elastic and, in many cases, serverless. Yet, organizations continue to attempt to operate security policies with controls that were not designed to dynamically scale and adapt instantaneously. To reconcile, security teams must conduct an increased amount of synchronization tasks and maintenance overhead.

2. **Virtualization Concentrates Risk**

   As applications and data become co-mingled, the attack surface becomes unwieldy as organizations struggle to manage policies and enforce least privilege. Under the guise of perimeter-based security, all users and administrators inside of the network are “trusted” with their access to cloud-based applications, regardless of whether or not privilege is properly maintained. Malicious actors use these oversights and management challenges to deliver a myriad of attack mechanisms. A single successful phishing attack of an authorized insider or spoofing an address can provide a foothold for attackers to move laterally within the network, and into the cloud for unfettered access to business critical data and applications.

Even though most modern networks are broken into “trust zones,” or segmented areas surrounded by access controls, these perimeters remain ineffective since attackers can gain enough information to piggyback on authorized network access policies.

3. **It’s Impossible to Protect What You Don’t Know**

   Cloud deployments remain opaque. Using traditional security tools with only a view through networking concepts like IP addresses, ports and payloads, security teams are crippled by blind spots. With a perimeter-focused security setup, the issue is compounded since a gap exists between what is enforced and what actually needs protecting. Attackers understand this weakness and exploit the gap to infiltrate, and then traverse through the network until they land on the intended target.

   The inability to properly secure or see into the network allows attackers to dwell for an average of over 200 days, despite best efforts. In that time, they have free range to deliver malicious payloads, establish presence and ultimately explore until they are ready to exfiltrate data.

Zero Trust – A More Effective Method

Traditional security constructs which relied on trusted addresses are giving way to the zero trust model in order to fix the perils of the new network paradigm. Through the guiding principle of “never trust, always verify”, it is assumed that the network is by default a hostile place, with not only external threats to deal with, but also internal. This shift in approach dictates that trust is only established once the secure identity of the applications, users and hosts controlling the addresses are authenticated. By allowing only trusted applications to communicate over approved network paths, organizations gain better security that extends beyond the network.

With reliance on homogenous security controls throughout the environment, zero trust allows for consistent policies, while remaining independent from the underlying network topology. As cloudfronts scale dynamically in real time, established controls and protection policies are able to adapt for instant, consistent security.

Edgewise Networks has embraced zero trust and has operationalized it with machine learning, for Trusted Application Networking. Using this approach, Edgewise Networks can stop compromise and attack progression of network-borne threats. To learn more about zero trust and how it is used as part of Trusted Application Networking, view our Zero Trust Networking 101 webinar.