Perimeter-based Network Security Strategy

Perimeter-based network security models date back to the early mainframe era (circa late 1950s), when large mainframe computers were located in physically secure “machine rooms” that could be accessed by only a relatively limited number of remote job entry (RJE) “dumb” terminals that were directly connected to the mainframe and also located in physically secure areas. Today’s data centers are the modern equivalent of machine rooms, but perimeter-based physical security is no longer sufficient for several obvious but important reasons:

Mainframe computers predate the internet. In fact, mainframe computers predate ARPANET, which predates the internet. Today, an attacker uses the internet to remotely gain access, instead of physically breaching the data center perimeter.

Data centers today are remotely accessed by millions of remote endpoint devices from anywhere and at any time. Unlike the RJEs of the mainframe era, modern endpoints (including mobile devices) are far more powerful than many of the early mainframe computers and are themselves targets.

The primary value of the mainframe computer was its processing power. The relatively limited data that was produced was typically stored on near-line media, such as tape. Today, data is the target. Data is stored online in data centers and in the cloud, and it is a high-value target for any attacker.

The primary issue with a perimeter-based network security strategy in which countermeasures are deployed at a handful of well-defined ingress and egress points to the network is that the strategy relies on the assumption that everything on the internal network can be trusted. However, this assumption is no longer safe to make, given modern business conditions and computing environments where:

Remote employees, mobile users, and cloud computing solutions blur the distinction between “internal” and “external”

Wireless technologies, the proliferation of partner connections, and the need to support guest users introduce countless additional pathways into the network branch offices that may be located in untrusted countries or regions

Insiders, whether intentionally malicious or just careless, may present a very real security threat

Perimeter-based approach strategies fail to account for:

The potential for sophisticated cyberthreats to penetrate perimeter defenses, in which case they would then have free passage on the internal network

Scenarios where malicious users can gain access to the internal network and sensitive resources by using the stolen credentials of trusted users

The reality that internal networks are rarely homogeneous but instead include pockets of users and resources with inherently different levels of trust or sensitivity that should ideally be separated in any event (for example, research and development and financial systems versus print or file servers)

A broken trust model is not the only issue with perimeter-centric approaches to network security. Another contributing factor is that traditional security devices and technologies (such as port-based firewalls) commonly used to build network perimeters let too much unwanted traffic through. Typical shortcomings in this regard include the inability to:

Definitively distinguish good applications from bad ones (which leads to overly permissive access control settings)

Adequately account for encrypted application traffic

Accurately identify and control users (regardless of where they're located or which devices they're using)

Filter allowed traffic not only for known application-borne threats but also for unknown ones

The net result is that re-architecting defenses in a way that creates pervasive internal trust boundaries is, by itself, insufficient. You must also ensure that the devices and technologies used to implement these boundaries actually provide the visibility, control, and threat inspection capabilities needed to securely enable essential business applications while still thwarting modern malware, targeted attacks, and the unauthorized exfiltration of sensitive data.