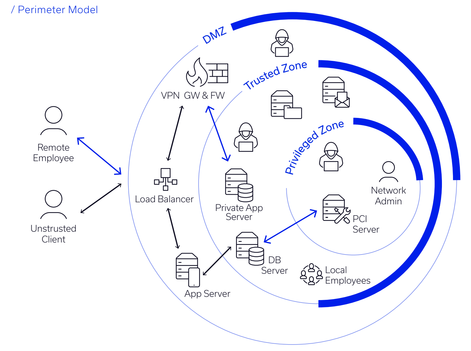
MAZEBOLT

5 Step Guide to **Zero Trust & DDoS**

Step One
Rethink Perimeter or Traditional Architecture

Perimeter or Traditional Architecture cannot prevent cyber attackers from accessing data or gaining control of critical systems.

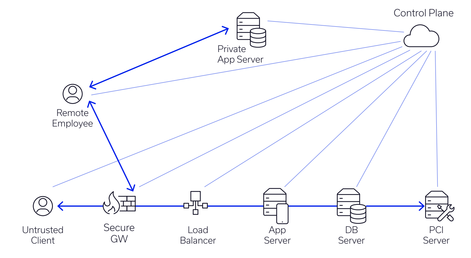
Traditional Network Architecture / Perimeter Model



Step Two
Move to the Zero Trust Model

The Zero Trust Model works on the principle that every network component is untrusted by default, in the network or outside of it.
An additional authentication layer is added and privileges to users are only given after authentication depending on their functions within the organization.

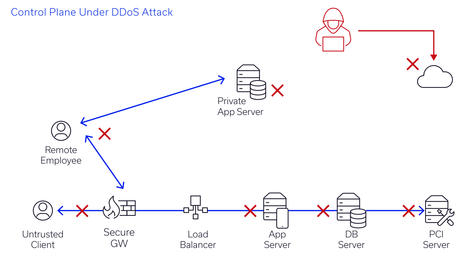
Zero Trust Architecture



Step Three
Understand Zero Trust's DDoS Failure Point

1. All controls, i.e., permissions and authentications are handled by a nerve center, i.e., `control plane'.
2. A DDoS attacker does not need to authenticate to communicate with a network.
3. The DDoS attacker sends malicious traffic to public network addresses.
4. When a flood of garbage traffic targets the network, the control plane can be overwhelmed.
5. When the control plane is down all communication comes to a halt.
6. The network has been brought down successfully.

Control Plane Under DDoS Attack



Step Four
Implement Zero Trust + DDoS Protection

1. Zero Trust will protect the organization from security breaches to sensitive systems and information.
2. DDoS protection that is validated 24/7 will keep the organization's online services and Zero Trust components protected and available.

24/7 protected&available

Step Five
Meet RADAR™

1. Detect, analyze, and prioritize remediation by automatically simulating more than 150 different DDoS attack vectors against every host in your network, 24/7 non disruptively.
2. Lower your network DDoS vulnerabilities level to under 2%.

To Know more about how to prevent DDoS attacks on a Zero Trust Model, download eBook `The CISO's Guide to DDoS Zero Trust' now.

Schedule Demo to see RADAR™ in action

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.