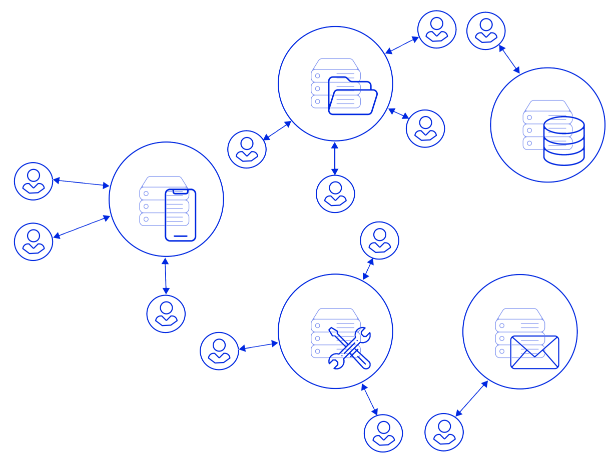
MAZEBOLT

Get Continuous DDoS Protection for Zero Trust Networks with No Downtime

Enterprise infrastructure has grown increasingly complex, with single enterprises increasingly supporting multiple networks, VPNs, and hybrid cloud and mobile environments. Ensuring security for such diverse, multi-layered, and fragmented resources have led to the wide-scale adoption of the Zero Trust (ZT) model.

The philosophy of Zero Trust is that assumptions of trust can prove to be disastrous for enterprise security and even a small error can lead to security breaches, and ultimately, revenue and customer loss.

HOW ZERO TRUST WORKS

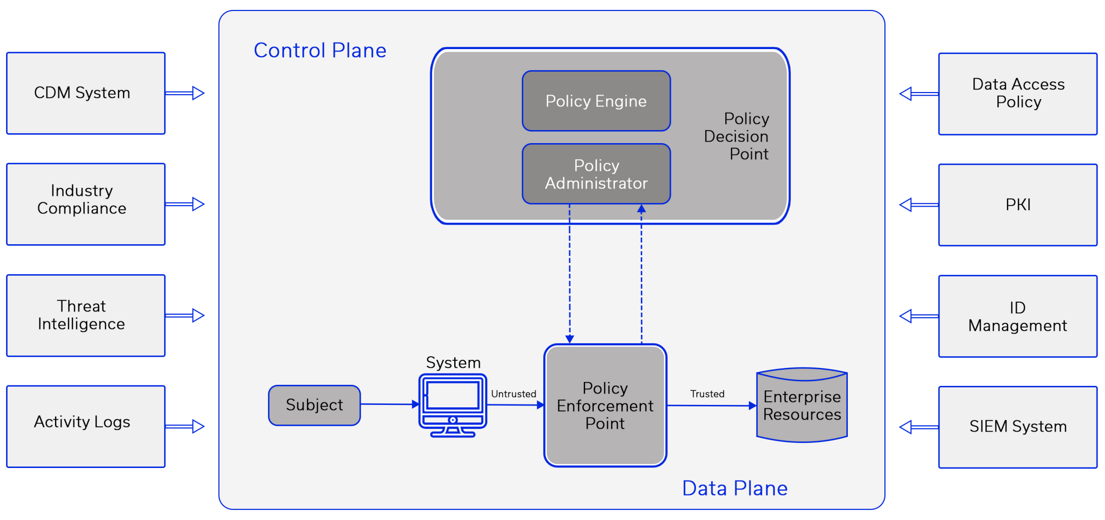


Zero Trust controls user access by requiring multiple authentications for different accesses. Authorization decisions for every access request in the network – for all devices and users – are made in the Control Plane.

The Control Plane consists of the Policy Engine (PE), Policy Administrator (PA) and the Policy Enforcement Point (PEP). The PE makes decisions related to user access while the PA executes these decisions. The PEP is responsible for enabling, monitoring, and eventually terminating connections.

WHY ZERO TRUST CANNOT PREVENT DDOS ATTACKS

Since the PA is the key component for resource access, enterprise resources cannot connect to each other without the PA's permission. If an attacker disrupts or denies access to the PEP(s) or PE/PA, no one can access anything on the network.

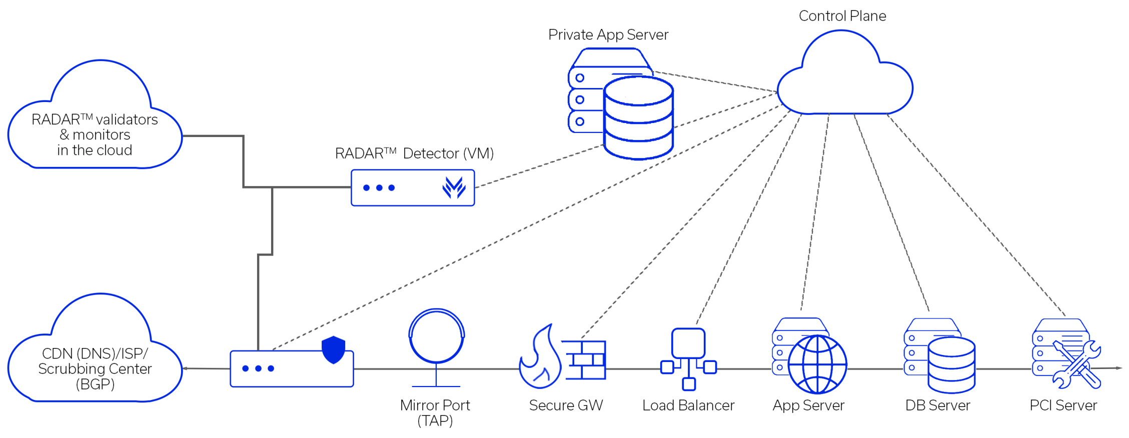


To summarize: If any of the components of the Control Plane are disrupted, legitimate users will be denied access to enterprise resources. In this case, a successful DDoS attack brings the network down.

ADOPT THE REVOLUTIONARY DDOS ZERO TRUST MODEL

The best solution for securing a network is to implement Zero Trust alongside a well-designed DDoS protection solution to defend organizations against security breaches to sensitive systems and information. Zero Trust protects the organization from security breaches of sensitive systems and information while DDoS protection validated 24/7 protects the Control Plane and maintains the security and availability of the organization's online services.

DDoS Zero Trust Model

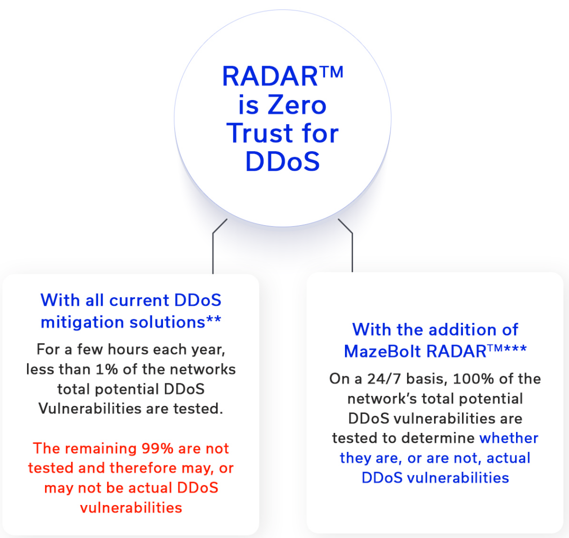


The only solution today in the market that can validate 24/7 is MazeBolt's patented DDoS RADAR™. RADAR™ is zero trust for DDoS because it follows the principle "trust your security but verify it." RADAR™ assumes everything is vulnerable unless proven otherwise.

RADAR™ validates that the network is well protected against DDoS attacks. It automatically simulates more than 150 different DDoS attack vectors against every host in a network,   24/7, with zero disruption (i.e., no system comes down or needs a maintenance window).

To know more visit:

www.mazebolt.com/radar.



RADAR™ is Zero Trust for DDoS

With all current DDoS mitigation solutions**

For a few hours each year, less than 1% of the networks total potential DDoS Vulnerabilities are tested.

The remaining 99% are not tested and therefore may, or may not be actual DDoS vulnerabilities

With the addition of MazeBolt RADAR™***

On a 24/7 basis, 100% of the network's total potential DDoS vulnerabilities are tested to determine whether they are, or are not, actual DDoS vulnerabilities

ABOUT MAZEBOLT

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

mazebolt.com | info@mazebolt.com