PROTECT AGAINST DENIAL OF SERVICE (DoS/DDoS) ATTACKS

With the proliferation of internet of things (IoT) devices, organizations are experiencing an increase in DoS and DDoS attacks, which not only disrupt business operations by affecting availability but also by degrading application performance. These attacks are notorious for being a smokescreen that is designed to distract organizations while hackers infiltrate the network through vulnerabilities in the environment.

As the DoS threat landscape continues to evolve in size, frequency, and complexity, DoS mitigation technologies need to make significant improvements to reduce dwell time. Armor's DoS solution integrates network-wide intelligence and anomaly detection with carrier-class threat management to help identify and stop volumetric, TCP state exhaustion, and application-layer DoS attacks.

Armor helps you tap the power of cloud computing without the complexity and cost of managing each core component on your own.

OUR SOLUTION

Armor's DoS/DDoS mitigation is a 24/7/365 service that significantly reduces negative effects on client environments. DoS/DDoS protection is provided at every datacenter location. DoS/DDoS mitigation detects probes and/or attacks including, but not limited to, operating system (OS) fingerprinting attempts, common gateway interface (C), buffer overflows, server message block (SMB) probes, and stealth port scans. Once an attack is identified, or sensed, based on abnormal behavior, the alert is logged and our security team effectively mitigates the threat.

ADDITIONAL LAYER OF DEFENSE AGAINST THREATS

Armor DoS/DDoS mitigation provides an extra layer of detection on your hosts to identify suspicious activity and alert you.

RANSOMWARE ADVANCED ANALYSIS & CORRELATION

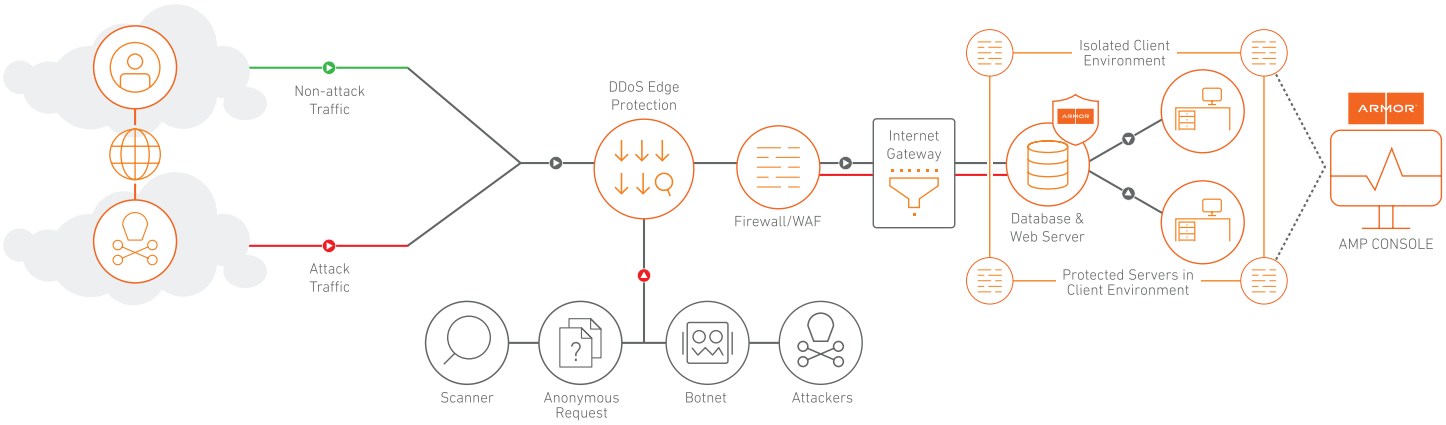
Events are analyzed and correlated with event data from your other devices under management by our threat prevention and response platform, delivering enhanced detection of potential threats across your public, private, or hybrid cloud—or on-premise—IT environments.

AUDIT-READY COMPLIANCE

Armor DoS/DDoS mitigation addresses key change control processes required by PCI DSS, HIPAA, HITRUST, SAN CSC, NIST, and other frameworks.

RESPONSE THAT GOES BEYOND ALERTING

Unlike traditional managed security service providers (MSSPs), Armor goes beyond simply alerting to a problem. Our security operations center (SOC) analysts monitor your environment 24/7/365 while they also work closely with your team to investigate and respond to potential incidents.



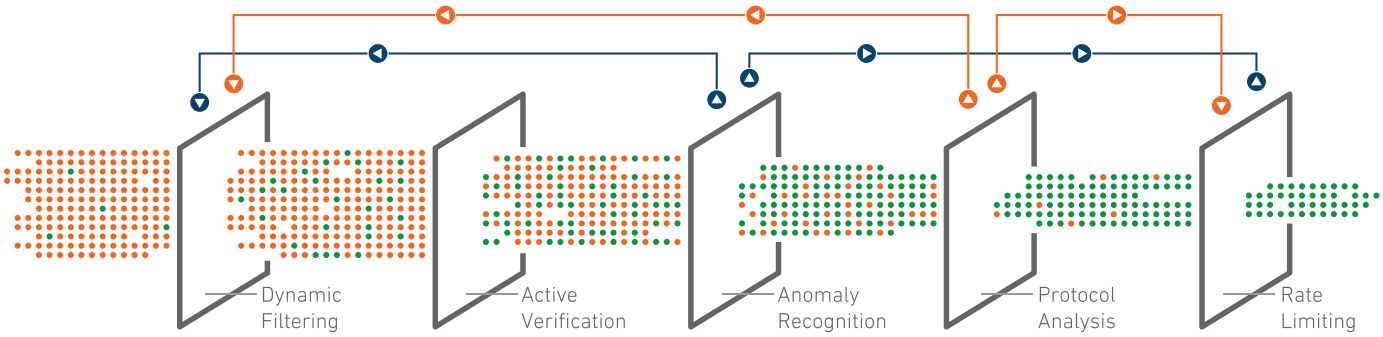
HOW DOES IT WORK?

A typical DoS/DDoS attack will not mirror normal traffic. It will be incongruous to expected traffic bandwidth. Generally, these anomalies are not a Dos/DDoS attack. In most cases, this is a misconfiguration of an application, client, or proxy—even the exploitation of a vulnerability on a server can cause some abnormal traffic patterns. Other times, it's a vulnerability or network scan that has gone unchecked and is scanning faster and with more concurrent requests than the site can process.

Armor deploys redundant, multi-stage DoS/DDoS mitigation systems within its infrastructure that provide early detection and mitigation for these types of attacks. These systems also connect automatically with upstream internet service providers for null routing efforts if necessary.

Block Actions	Source blocking/source suspend; per packet blocking; combination of source, header, and rate-based blocking		
Attack Protections	**Flood Attacks** TCP, UDP, ICMP, DNS,SSDP, NTP, SNMP, SQL RS, charge amplification, DNS amplification, Microsoft SQL resolution service amplification, NTP amplification, SNMP amplification, and SSDP amplification	**Application Attacks** HTTP GET floods, SIP invite floods, DNS attacks, HTTPS protocol attacks, DNS cache poisoning, vulnerability attacks, resource exhaustion attacks (Slowloris, Pyloris, and LOIC)	**Fragmentation Attacks** Teardrop, Targa3, Jolt2, Nestea **TCP Stack Attacks** SYN, FIN, RST, SYN ACK, URG-PSH, TCP flags **Flash Crowd Protection** IPv4/IPv6 attacks hidden in SSL encrypted packets
DoS/DDoS Counter-measures	Invalid packets, IPv4/IPv6 address filter lists, IPv4/IPv6 black/white filter lists, packet header filtering, IP location filter lists, zombie detection, per connection flood protection, TCP SYN authentication, TCP connection, limiting TCP connection reset	Payload regular expression filter, shaping, IP location policing, inline filter, blacklist fingerprints, protocol baselines, HTTP authentication, HTTP malformed, HTTP scoping, HTTP rate limiting	HTTP authentication, HTTP malformed, HTTP scoping, HTTP rate limiting, HTTP/ URL regular expression, DNS authentication, DNS malformed, DNS scoping, DNS rate limiting, DNS regular expression, SIP malformed, SIP request limiting, SSL negotiation, ATLAS intelligence feed (AIF)

Anomaly recognition and protocol analysis update the dynamic filtering and rate limiting modules in real time to block newly identified attack traffic.



DoS/ DDoS mitigation and service enhances our Armor managed security-as-a-service (SECaaS) and Armor Complete secure hosting (Optional) solutions to provide total security protection across your entire security stack.

MAINTAIN SECURITY POSTURE AND COMPLIANCE

Armor does more than secure the network. Our experts monitor and secure your hosts. A defense-in-depth solution that secures your operating system up to the application layer.

Armor's DoS/DDoS mitigation service automatically assesses and understands risk across your entire infrastructure offering:

- Fully managed, tightly integrated combination of in-cloud and on-premise DoS/DDoS protection
- 24/7/365, in-line, detection and mitigation of DoS/DDoS attacks ranging from sub 100Mbps to 40Gbps
- Cloud signaling, which provides intelligent integration with Armor Cloud
- Availability as an appliance or virtual platform with optional managed service
- Capability to stop inbound and outbound DoS/DDoS attacks and malware

LEARN MORE

Click to learn more about **Armor** or **Armor Complete**.

POWERED BY THE ARMOR PLATFORM

Armor DoS/DDoS mitigation service is powered by our platform—the IT security industry's leading threat prevention and response platform. We integrate advanced analytics, global threat intelligence, and continuous response capabilities into a single platform that bolsters your defenses, uncovers hidden threats, and prevents security breaches. Whether your sensitive data and workloads are stored in a private, public, or hybrid cloud—or in an on-premise IT environment, Armor provides a proactive approach to cyberthreats.

OPTIMIZED FOR

aws

Microsoft Azure

Google Cloud

vmware

ARMOR