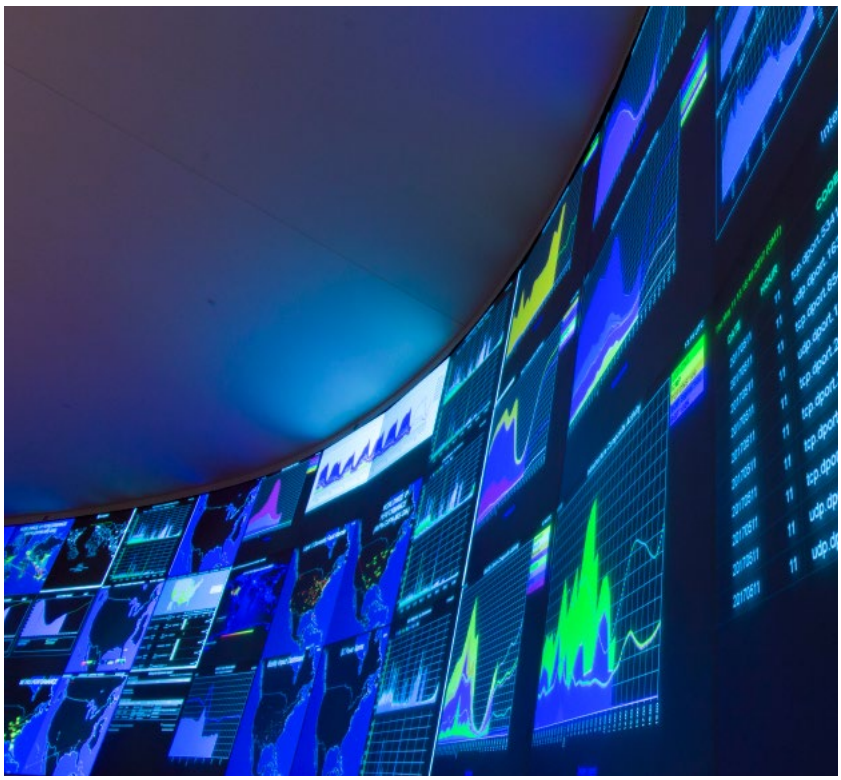
AT&T Business

Stop DDoS attacks in their tracks



Distributed Denial of Service (DDoS) attacks are among the most disruptive and vicious cyberthreats to businesses today. Potentially system crippling, they undermine your customer service and brand equity while potentially taking large bites out of your revenue.

Potential benefits

- Helps stop DDoS attacks before they overwhelm your network
- Assists in maintaining information availability internally and externally
- Helps to protect your internal network from unauthorized activities
- Gives you a proactive defense posture so you're prepared to deal with DDoS attacks
- Provides visibility to network status with advisories, critical alerts, and attack notifications

Features

- Monitors for threats over specified IP address range
- Detects the presence of an identified DDoS attack
- Provides anomaly detection, packet scrubbing, traffic analysis, and e-mail trap alerts
- Includes web portal access for service and status reporting

1 Defend proactively

Keep your guard up. The early warning capabilities of AT&T DDoS Defense (proactive) help you stop attacks before they overwhelm your network. With 24/7 resource monitoring by one of our detection facilities, we can identify threats and begin mitigation while the attack is in its infancy.

2 Scrub the attack

Cripple the DDoS attack before it cripples you. During an attack, AT&T DDoS Defense can automatically divert all traffic from the targeted server to a scrubbing facility. There, we filter out DDoS attack traffic and push valid traffic through to your access router.

3 Analyze and act

Continuously prepare for the next strike. Through a specialized web portal, you can gain insights on network status, attack reports, and service updates.

Protect your business with AT&T DDoS Defense

AT&T DDoS Defense adds a key layer to your cybersecurity defense strategy. With cybersecurity measures set in place and managed by the world's largest integrated communications provider, you build a foundation for your business that can help contain risk, embrace change, and elevate trust. Help protect your network and servers, and stop attacks before they impact your business.

Enhance protection with cloud signaling

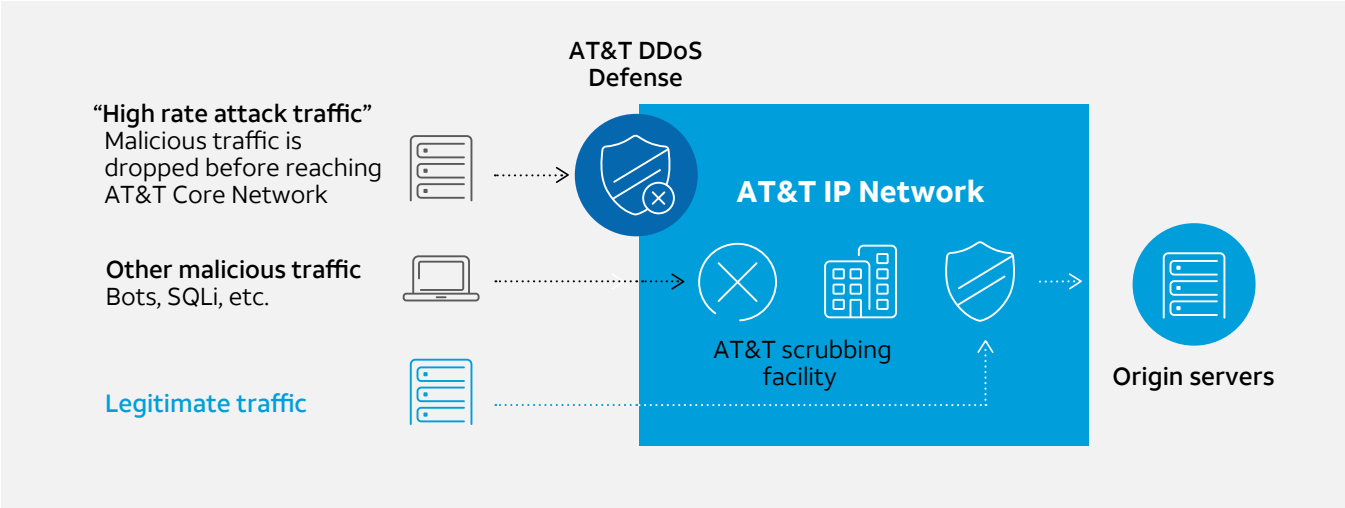
As a support feature available to AT&T DDoS Defense service customers, cloud signaling allows your service to accept alerts from premises-based devices in the form of cloud signals. In the event of application layer or smaller DDoS attacks, using cloud signaling, traffic can be rerouted to the AT&T DDoS Defense service for cloud based mitigation.

Add layers of security with AT&T Secure Network Gateway

You can get AT&T DDoS Defense as a stand-alone service or as part of AT&T Secure Network Gateway service—a suite of products and services that adds layers of security to your cyberdefense. It delivers state-of-the-art security features with proactive monitoring and management.

We have simplified the purchasing, contracting, and billing of specific components of AT&T Secure Network Gateway service: AT&T DDoS Defense (proactive or reactive), AT&T Network-Based Firewall service, AT&T Secure E-mail Gateway service, and AT&T Web Security service. You can get them under one contract and one invoice.

How AT&T helps protect against DDoS attacks



AT&T Business

Top readiness tips to help keep you prepared	
Getting ready for a DDoS attack	• Have a reaction plan ready to implement. • Document the key technical players to help remediate an attack. Use small task forces to make good decisions quickly. • Depending on the level of service chosen, allow for testing of the anti-DDoS service annually and see to it that all notifications are received as expected. • Engineer network components and other resources to accommodate attack scenarios above and beyond normal, anticipated loads. • Keep mitigation settings current with gateway architecture (i.e. circuits, IP addresses, servers, services). • Be sure your anti-DDoS attack Service Provider is experienced and well versed in current attack vectors. • Understand the ISP's capabilities for dealing with attacks. • Prepare an alternate form of communication during an attack in the event that other IP based services are impacted i.e. VoIP, e-mail. • Understand and document the gateway architecture as it evolves and know how to implement routing changes quickly.
During a DDoS attack	• Refer to the documented plan. • Document all mitigation/corrective steps taken. • Save logs and packet captures for post mortem reviews.
Threat landscape	• Attackers' motives include political agendas, financial gains, and bragging rights. Every business is susceptible to an attack. • A DDoS attack is often a diversionary tactic to enable other illicit activities such as data theft or fraud. • All attacks are different – some are volumetric in nature while others exploit Transmission Control Protocol Layer 7 vulnerabilities. Yet some attacks exploit both. • Attackers tend to change their tactics and adapt to defensive measures put into place.

Why AT&T

Our edge-to-edge technologies enhance your networks, infrastructure, and devices with managed cybersecurity products and services to help protect your business.

For more information about AT&T DDoS Defense, visit us at https://www.business.att.com/products/ddos-protection.html or call us at 877.219.3898.

Share this with your peers