

Proactively protect against volume- based attacks

AT&T Distributed Denial of Service (DDoS) Defense

DDoS attacks cost time and money.

More than ever, Distributed Denial of Service attacks are among the most disruptive and vicious activities passing over the Internet.




Malicious hackers launch **more than 7,000** Distributed Denial of Service (DDoS) attacks each day.

DDoS attacks overwhelm web servers and saturate your agency's internet connections, web servers and firewalls.

DDoS attacks are designed to disable infrastructure resources and applications, causing loss of productivity as well as damage to an agency's image, and reputation.

Introducing AT&T DDoS Defense Service

AT&T DDoS Defense Service provides cloud-based monitoring of and protection against volumetric distributed denial of service attacks. Detailed traffic analysis helps to identify anomalies, so that malicious traffic can be sent to scrubbing facilities and blocked.

Detect	Mitigate	Control
		
Helps to quickly identify attacks	Mitigates a broad range of attacks	Allows legitimate traffic to reach your servers
24x7 monitoring and alerts by a team of cybersecurity experts helps identify threats.	Rapid implementation of a predefined plan, built around your preferences and based on our vast threat intelligence.	Scrubbing facilities around the world, filter out malicious packets

How prepared is your agency?

- 1 What would happen if your mission critical, public facing server is unavailable due to a DDoS attack?
- 2 Do you have a plan in place to mitigate a large scale attack?
- 3 What does your protocol say about responding to a ransom note threatening to unleash a DDoS attack within 24 hours?
- 4 Do you know what your options are?
- 5 How long could your agency weather the impact of a serious security breach with effects such as?:



Lost PII data



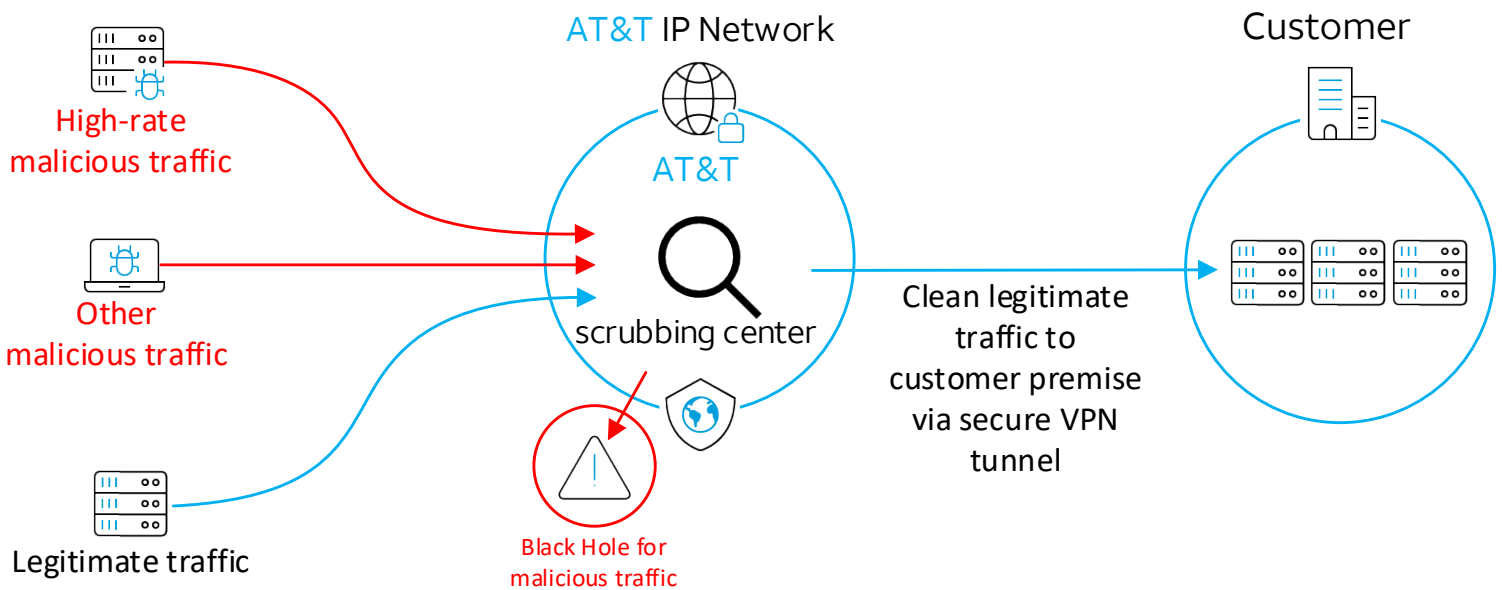
Encrypted data



Connectivity outages

Routing traffic through the AT&T Virtual Private Network (VPN) delivers clean traffic to the AT&T edge providing protection from Internet-facing exposures.

Detect	Mitigate	Control
Black holes help stop bad traffic at the Network Edge, before reaching the AT&T Core Network	Malicious traffic (Botnets, etc.) is identified and scrubbed in AT&T Cloud before reaching customers	Legitimate traffic flows to customers



The Benefits

AT&T DDoS Defense can help to **proactively mitigate volumetric DDoS attacks** before they reach an agency's network and disrupt their activity.



**Global
Visibility**



**Proactive
Protection**



Simplicity

Defend against threats and volumetric attacks with always monitored data flows, a global view of the threat landscape, and an early warning system.

Help to proactively mitigate attacks before they reach your network, including the ability to drop attack packets at the AT&T network edge.

Blocks malicious packets in real time while allowing the flow of legitimate traffic.

Simple activation and operation, enables agencies to deploy powerful security with zero downtime.

Provides a robust, information security portal with web portal access for service and status reporting, including anomaly reporting, historical archiving, and dark address analysis.