

Managed DDoS Defense

Comprehensive DDoS protection delivered as a fully managed solution.

Organizations across industries are under pressure as DDoS attacks grow in frequency, sophistication, and scale. A proactive defense ensures attacks are stopped before they disrupt operations, keeping your business resilient and your customers connected.

LevelBlue Managed DDoS Defense

LevelBlue Managed DDoS Defense helps safeguard against the largest, most complex DDoS attacks in the world with 24x7 monitoring and mitigation, ensuring operational resilience and business continuity for clients.

One of the world's largest cybersecurity service providers, LevelBlue tailors its service to the unique industry and business requirements of a client, including small to large enterprises, state and local governments, and federal agencies. The LevelBlue DDoS Operations team can begin mitigating within five minutes of suspecting an attack. Our DDoS specialists identify the nature of an attack and provide mitigation options, using the same infrastructure that AT&T uses to protect its own network.

Protection against volumetric attacks

LevelBlue Managed DDoS Defense continuously monitors a client's in-scope IP addresses via network-based detection, proactively searching for unusual network traffic patterns, spikes in request volume, and other anomalies that indicate a precursor to a DDoS attack. During mitigation, LevelBlue reroutes a client's incoming traffic to scrubbing centers, separating and containing malicious packets and forwarding legitimate traffic. This process occurs in near real time. LevelBlue continues to reroute and scrub the traffic until the attack subsides, after which LevelBlue restores normal traffic routing (see figure 1). In parallel, the LevelBlue DDoS Operations Team analyzes the attack to augment response and directly communicates with the client.

Why LevelBlue Managed DDoS Defense?

- Get 24x7 monitoring and mitigation through our global DDoS Defense Operations
- Take advantage of LevelBlue's 20+ years of experience with DDoS traffic analysis and attack assessment
- Stop DDoS attacks using the same infrastructure that protects AT&T's network
- Get visibility, insight, and reporting via the DDoS Defense customer portal, including network status and critical alerts
- Use anomaly detection, packet scrubbing, traffic analysis, and e-mail trap alerts for proactive defense
- Upgrade to expedited turn-up, customized IP addresses or ranges for monitoring and mitigation, enhanced reporting, and dedicated support

1 Defend Proactively

Stop attacks before they overwhelm your network, with 24x7 monitoring and early warning capabilities. LevelBlue identifies threats and begins mitigation while the attack is in its infancy.

2 Scrub the Attack

During an attack, LevelBlue DDoS Defense diverts all traffic from the targeted asset to a scrubbing facility. There, LevelBlue filters out DDoS attack traffic and forwards valid traffic through to your access router.

3 Analyze the Attack

The LevelBlue DDoS Operations Team provides expert mitigation guidance and 24x7 responsiveness to ensure the most sophisticated attacks are addressed quickly. The DDoS Defense customer portal offers insight on network status, attack reports, and service updates.

Service tiers

LevelBlue offers flexibility with three Managed DDoS Defense service tiers: Essentials, Advanced, and Premium. Clients choose the level of service that best meets their requirements and budget. The Essentials tier offers 24x7 foundational protection and automatic or client-approved response. The Advanced tier adds faster response and actionable insight, and the Premium tier provides highly tailored, granular protection, strategic assessment and improvement, and service coverage for multiple carriers. Across all tiers, clients reduce risks associated with DDoS attacks through faster recovery times and actionable insights that help to continuously improve the organization's security posture and ensure adherence to compliance mandates.

Service Component	Essentials	Advanced Essentials capabilities plus	Premium Advanced capabilities plus
Monitoring and Detection	<ul style="list-style-type: none"> 24x7 with traffic analysis 	<ul style="list-style-type: none"> 24x7 with traffic analysis 	<ul style="list-style-type: none"> 24x7 with traffic analysis
LevelBlue DDoS Defense Customer Portal	<ul style="list-style-type: none"> Portal and training included 	<ul style="list-style-type: none"> Portal and training included 	<ul style="list-style-type: none"> Portal and training included
Service Activation	<ul style="list-style-type: none"> Standard service activation (2-4 weeks) Biannual DDoS readiness tests 	<ul style="list-style-type: none"> Expedited service activation (5 business days) Quarterly DDoS readiness tests 	<ul style="list-style-type: none"> Expedited service activation (5 business days) Quarterly DDoS readiness tests
Protection Zones and Customization	<ul style="list-style-type: none"> One regional protection zone 	<ul style="list-style-type: none"> One regional protection zone 	<ul style="list-style-type: none"> One regional protection zone Up to 5 sub zones with granular IP monitoring Up to 5 sub zones with granular IP mitigation Carrier-agnostic protection (up to 2 non-AT&T circuits within the U.S.)
Response and Mitigation	<ul style="list-style-type: none"> Automatic mitigation within 30-minutes of attack detection* 	<ul style="list-style-type: none"> Automatic mitigation within 5-minutes of attack detection* 	<ul style="list-style-type: none"> Automatic mitigation within 5-minutes of attack detection*
Reporting	<ul style="list-style-type: none"> Self-service reports via the customer portal 	<ul style="list-style-type: none"> Monthly report sent by the DDoS Operations Team 	<ul style="list-style-type: none"> Monthly report sent by the DDoS Operations Team
Service Support	<ul style="list-style-type: none"> 24x7 on-demand support 	<ul style="list-style-type: none"> 24x7 on demand support Monthly operational meeting 	<ul style="list-style-type: none"> 24x7 on demand support Monthly operational meeting
Dedicated DDoS Engineer			<ul style="list-style-type: none"> Dedicated engineer for advisory and support Biannual technical meeting
Add-on Options			
Platform-Initiated Mitigation Object	Add on available	Add on available	Add on available
Carrier-Agnostic Protection (U.S. Only)	Add on available	Add on available	Add on available
Expedited Activation	Add on available		
Emergency Deployment	Add on available	Add on available	Add on available

How LevelBlue helps protect against DDoS attacks

