LevelBlue

SERVICE BRIEF

LevelBlue Managed DDoS Defense

Distributed denial of service (DDoS) attacks are growing in frequency, sophistication, and scale, targeting organizations of all sizes and across industries. In parallel, organizations face a growing set of challenges when it comes to DDoS protection, including an expanding DDoS attack surface, limited staff, budget, or technical knowledge to support 24/7 DDoS monitoring and protection, and increased regulatory pressure. To meet these challenges, security leaders realize they need to implement proactive DDoS defense measures, however, they need help.

LevelBlue Managed DDoS Defense

LevelBlue Managed DDoS Defense helps safeguard against the largest, most complex DDoS attacks in the world with 24/7 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.

1 DEFEND PROACTIVELY	2 SCRUB THE ATTACK	3 ANALYZE AND ACT
Stop attacks before they overwhelm your network, with 24/7 monitoring and early warning capabilities. LevelBlue identifies threats and begins mitigation while the attack is in its infancy.	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.	The LevelBlue DDoS Operations Team provides expert mitigation guidance and 24/7 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.

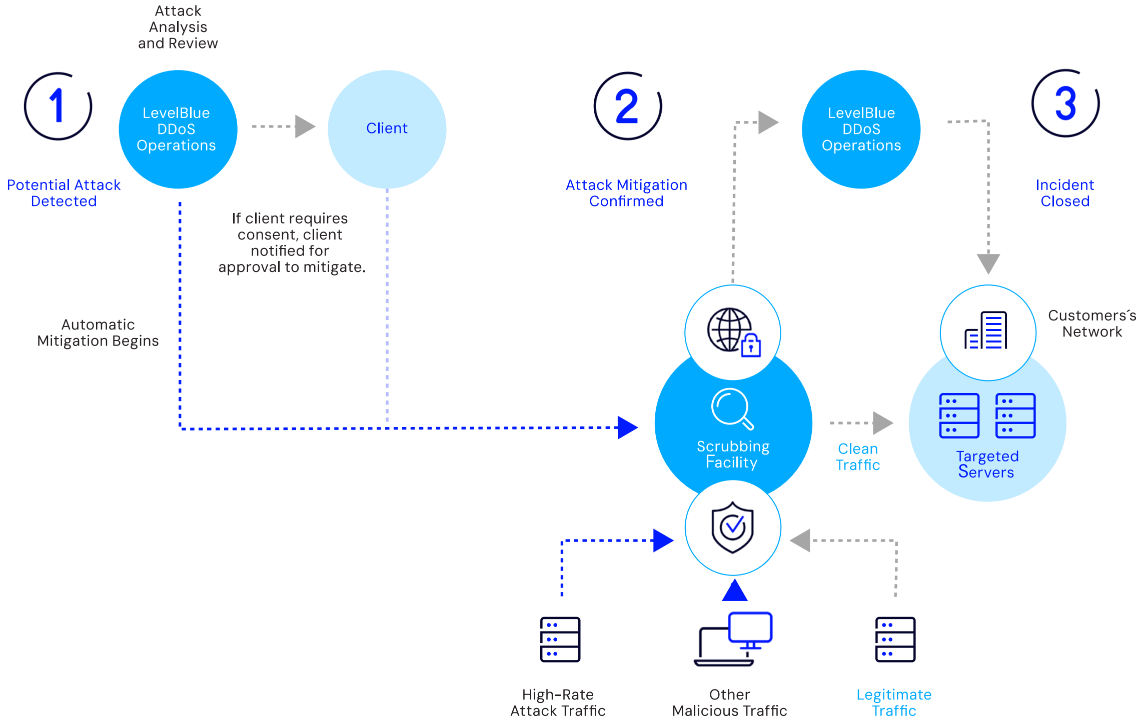
Protection Against Volumetric Attacks

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.

LevelBlue DDoS Defense 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 24/7 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.


Attack Analysis and Review
1
LevelBlue DDoS Operations
Client
Potential Attack Detected
If client requires consent, client notified for approval to mitigate.
Automatic Mitigation Begins
2
Attack Mitigation Confirmed
LevelBlue DDoS Operations
3
Incident Closed
Customers's Network
Scrubbing Facility
Clean Traffic
Targeted Servers
High-Rate Attack Traffic
Other Malicious Traffic
Legitimate Traffic

LEVELBLUE MANAGED DDOS DEFENSE			
	ESSENTIALS	ADVANCED	PREMIUM
Monitoring and Detection	• 24/7 with traffic analysis	• 24/7 with traffic analysis	• 24/7 with traffic analysis
LevelBlue DDoS Defense Customer Portal	• Portal and training included	• Portal and training included	• Portal and training included
Service Activation	• Standard service activation (2-4 weeks) • Biannual DDoS readiness tests	• Expedited service activation (5 business days) • Quarterly DDoS readiness tests	• Expedited service activation (5 business days) • Quarterly DDoS readiness tests
Protection Zones and Customization	• One regional protection zone	• One regional protection zone	• 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	• Automatic mitigation within 30-minutes of attack detection*	• Automatic mitigation within 5-minutes of attack detection*	• Automatic mitigation within 5-minutes of attack detection*
Reporting	• Self-service reports via the customer portal	• Monthly report sent by the DDoS Operations Team	• Monthly report sent by the DDoS Operations Team
Service Support	• 24/7 on-demand support	• 24/7 on-demand support • Monthly operational meeting • Dedicated Microsoft Teams meeting space	• 24/7 on-demand support • Monthly operational meeting • Dedicated Microsoft Teams meeting space
Dedicated DDoS Engineer			• 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 (United States 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

- * Client may elect to require explicit approval to proceed with mitigation for any tier. Client-approved mitigation starts within 30-minutes of client consent

LevelBlue Managed DDoS Defense Service Components

Monitoring and Detection

Get 24/7 monitoring of incoming and outgoing network traffic and real-time traffic analysis to identify abnormal or irregular traffic patterns that indicate malicious activity. Provides early detection and rapid response to prevent network downtime, preserve bandwidth, and ensure uninterrupted access for legitimate users.

LevelBlue Managed DDoS Defense Customer Portal

Use the portal for centralized account administration, including change requests and reports. Gain visibility of protection zones and monitor, add, or remove IP addresses under protection. Monitor account activity and mitigation details, including for applications, UDP and TCP communications, top account activity, and alerts.

Service Activation

Activate DDoS Defense within as little as five business days. Activation includes advisory to identify and designate protection zones and sub zones, technical provisioning support, documentation of client contacts and response requirements, service deployment and testing, baseline traffic-flow patterns, and DDoS readiness testing. LevelBlue also offers emergency activation and attack mitigation for organizations in an active DDoS attack.

Emergency DDoS service activation is also available.

Onboarding and Training: Get comprehensive training on the DDoS Defense customer portal, including instructions on how to navigate analytics, set up user profiles, and interpret reports.

DDoS Readiness Testing: Request up to four readiness tests annually, depending on the service tier. LevelBlue simulates a DDoS attack to validate the effectiveness of defenses and response, assessing critical functions, mitigation capabilities, and confirming that legitimate traffic can still flow to your network during an attack.

Protection Zones and Sub Zones

Designate specific protection zones with broad IP address coverage for a select region (United States and parts of Canada, Europe excluding Russia, and Asia-Pacific). Tailor monitoring and response with sub zones for a specific set or range of IP addresses within a protection zone. Leverage up to five monitoring objects and up to five platform-initiated mitigation objects to create sub zones.

Monitoring objects provide for in-depth monitoring of traffic flows and patterns.

Platform-initiated mitigation objects enable more granular alert and mitigation thresholds for detecting unusual traffic patterns, spikes in request volume, or other anomalies that indicate a precursor to an attack.

Response and Mitigation

Automatic Mitigation: Speed response with automatic mitigation for protected zones and sub zones (sub zones are managed via platform-initiated mitigation objects with specific mitigation thresholds). Automatic mitigation is initiated when designated traffic volumes are exceeded or an attack is detected (within 30 minutes for Essentials and 5 minutes for Advanced and Premium).

Client-Approved Mitigation: Require explicit approval before attack mitigation begins. Mitigation is initiated within 30 minutes of client consent.

Why LevelBlue?

- Get 24/7 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

Carrier-Agnostic Protection

Extend monitoring and mitigation to AT&T and non-AT&T circuits for multi-carrier environments (with /24 netblock or larger).

Reporting

Get actionable intelligence and detailed reporting to informa decisions and improve your security posture.

Self-Service Reports: Access standard reports, including real-time traffic insights, anomaly detection, and historical data via the LevelBlue DDoS Defense customer portal.

Proactive Monthly Reporting: Get detailed monthly summaries of alerts, mitigations, and traffic patterns tailored for executive-level reviews (sent by the DDoS Operations Team).

Service Support

Stay informed by engaging with the DDoS Defense Operations Team to continuously improve your service and ensure alignment with your organization's network changes and security objectives.

24/7 Operational Support: Get 24/7 access to cybersecurity experts via phone or email.

Monthly Operations Meeting: Take advantage of a monthly operational meeting to review account activity, including traffic patterns, alerts, mitigations, client contacts changes, and DDoS attack trends and insights.

Dedicated Microsoft Teams Meeting Space: Access a dedicated Microsoft Teams group to streamline communication, securely share files, and engage directly with LevelBlue's DDoS experts in real time.

Dedicated DDoS Engineer

Secure a dedicated DDoS engineer who provides personalized expertise and tailored recommendations to improve safeguards against evolving DDoS attacks and attacks you are susceptible to.

Biannual Engineering Meeting

Leverage expert insights to optimize your DDoS protection, refine strategies, and stay ahead with performance analysis, incident reviews, and emerging trend updates.

Enhance Protection with LevelBlue Managed Web Application and API Protection (WAAP)

LevelBlue Managed DDoS Defense clients can enhance protection with additional services, including Managed Web Application and API Protection (WAAP) for robust application-layer attack defense.

Clients can also leverage consulting services for in-depth security assessments and tailored support for DDoS implementation and mitigation strategies.

Learn More

If you are interested in learning more or immediately activating DDoS protection, contact your LevelBlue representative. Organizations can also reach out through the LevelBlue website.

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

For more information about LevelBlue Managed DDoS Defense, visit us at LevelBlue.com.