LevelBlue

PRODUCT BRIEF / JUNE 2024

Stop DDoS Attacks in Their Tracks

Distributed Denial of Service (DDoS) attacks are among the most disruptive and vicious cyberthreats to agencies today. Potentially system crippling, they can cause irreparable damage to government organizational functions and reputation, impacting network operations, public transactions, and public and industry data access.

1 Defend Proactively

Keep your guard up. The early warning capabilities of LevelBlue 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, LevelBlue 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.

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 streamlined web portal access—providing network telemetry and analytics for inbound/outbound traffic, data spike alerts, mitigation oversight, and tunable Protected Zones

LevelBlue

Protect Your Agency with LevelBlue DDoS Defense

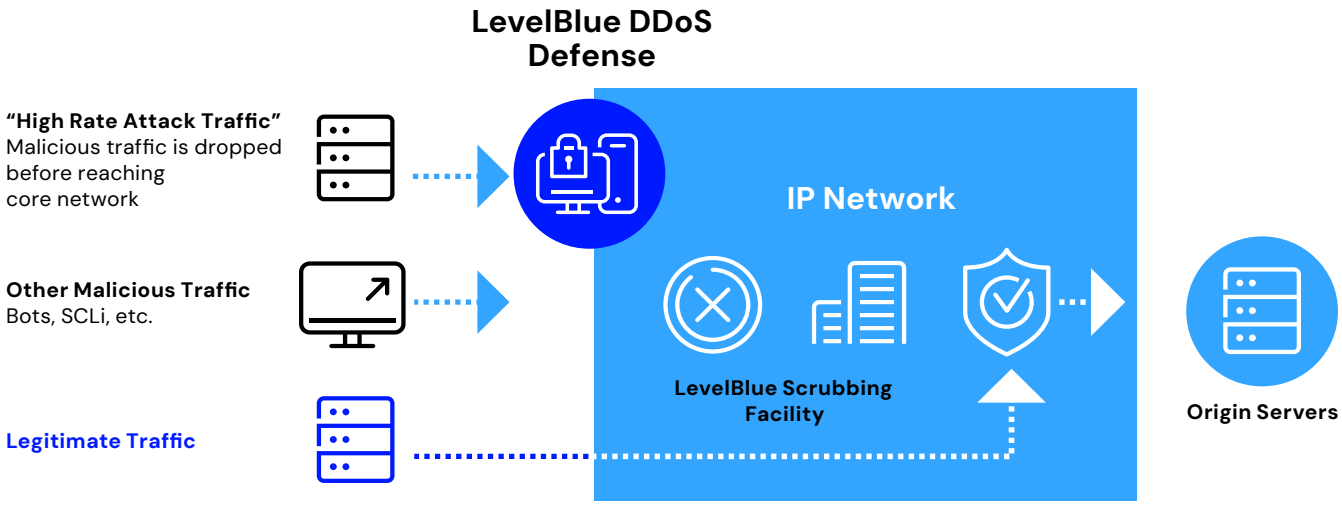
LevelBlue DDoS Defense adds a key layer to your cybersecurity defense strategy. With cybersecurity measures set in place and managed by you, build a foundation for your agency that can help contain risk, embrace change, and elevate trust. Help protect your network and servers, and stop attacks before they impact your agency. LevelBlue supports a number of public sector contracting vehicles for SLED including NASPO and state specific contract formats.

Add Layers of Security with LevelBlue Secure Network Gateway

You can get LevelBlue DDoS Defense as a stand-alone service or as part of LevelBlue 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 LevelBlue Secure Network Gateway service: LevelBlue DDoS Defense (proactive or reactive), LevelBlue Network-Based Firewall service, LevelBlue Secure E-mail Gateway service, and LevelBlue Web Security service. You can get them under one contract and one invoice.

How LevelBlue Helps Protect Against DDoS Attacks



Stop DDoS Attacks in Their Tracks

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 agency 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. • Talk to your sales representative about how LevelBlue can integrate layer 3 and 4 DDoS Defense with Layer 7 web and application protection.

LevelBlue

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 DDoS Defense, visit us or call us at 877.219.3898