LevelBlue

PRODUCT BRIEF / MAY 2024

React Quickly to DDoS Attacks and Shut Them Down

If not acted upon quickly, Distributed Denial of Service (DDoS) attacks can be extremely disruptive to your business. It's important to have a contingency plan. LevelBlue Reactive DDoS Defense service is that contingency plan.

React quickly

Time is of the essence. That's why our dedicated 24/7 LevelBlue Threat Management center is here for you. When you know your servers are under attack, simply call to enact the prompt and effective mitigation process that helps stop the attack before it overwhelms your network.

Scrub the attack

Divert traffic destined to the attacked IP address(es) to our scrubbing facilities. While the offending packets are cleaned, valid traffic will still be forwarded to your network via an internal VPN link. This helps minimize the impact of the attack, and lets you continue to serve clients and conduct transactions.

Analyze and act

Continuously prepare for the next strike. Through a specialized web portal, review details about previous attacks to identify potential areas that could be fortified.

Potential benefits

- Helps to protect your internal network from unauthorized activities
- Gives you a 24/7 threat response plan to defend your company from DDoS attacks
- Provides visibility into attack and mitigation details

Features

- Gives access to 24/7 LevelBlue Threat Management center
- Mitigates threats over specified IP address range
- Includes web portal access for service and status reporting

Be prepared with LevelBlue Reactive DDoS Defense

In a world of constantly evolving threats, LevelBlue Reactive DDoS Defense service gives you a safety net. With cybersecurity measures set in place and managed by you, build a foundation for your business that can help contain risk, embrace change, and elevate trust.

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.
- Contact your anti-DDoS attack Service Provider for assistance.
- 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.

For more information about Reactive DDoS Defense, visit us at www.LevelBlue.com or call us at 877.219.3898

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.