



DDoS Readiness

An Akamai Professional Services Solution

To combat distributed denial-of-service (DDoS) attacks launched by botnets and other malicious code, enterprises need a multi-layered defense architecture that extends visibility and control to the edge of the network. Situated between end-user requests and the enterprise's core infrastructure, the Akamai platform can uniquely provide critical layers of defense as part of a comprehensive security strategy.

Gain Peace of Mind in an Uncertain World

As enterprises continue to push business critical data and operations into the Cloud, they must take appropriate measures to protect these assets from the growing threat of sophisticated and motivated adversaries. The chaos and downtime associated with outages caused by DDoS attacks – and the post-incident steps required to recover – can be a significant resource drain.

The Akamai DDoS Readiness solution helps customers prepare for, monitor, manage, and mitigate the impacts of malicious DDoS attacks. By combining the industry expertise of seasoned Akamai consultants with Akamai's sophisticated solutions, the DDoS Readiness service helps you anticipate and alleviate common and uncommon DDoS threats. Plus, when bought with Akamai's DDoS Fee Protection service, you can mitigate the financial risks associated with traffic bursting fees.

Through DDoS Readiness, Akamai Professional Services will:

- 1 | Review your site for DDoS readiness and provide a detailed assessment including recommendations.
- 2 | Develop customer-specific DDoS incident response procedures, for use during a DDoS attack.
- 3 | Conduct After Action Report of each DDoS event to help you plan for and minimize the risk of future attacks.

Be Prepared for Anything

This comprehensive package provides everything you need to prepare for traffic spikes, monitor and report on site performance during a DDoS event, and gain a thorough understanding of how you performed so you can best guard against future attacks.

BENEFITS TO YOUR BUSINESS

- Maximize availability, even during DDoS attacks
- Protect your brand reputation
- Understand the attack profile after an event
- Gain peace of mind by leveraging best-in-class guidance, expertise, and support

CONTACT AKAMAI TODAY

Interested in learning more about DDoS Readiness? Contact your sales representative today.

Preparation Before a DDoS Attack

It's often said that preparation is 80% of execution. With that in mind, Professional Services will perform a readiness assessment identifying Akamai best practices you can employ online to withstand a DDoS attack. Dedicated to ensuring you maintain a strong security posture, our experts will share insights and best practices gleaned in the course of helping leading institutions succeed online – so you can be confident about your security architecture.

Deliverables:

1. Report including recommended configuration changes designed to bolster security
2. Standard Operating Procedures (SOP) that define stakeholder roles and actions for both Akamai and your organization during a DDoS attack
3. Alert setup assistance
4. EdgeControl portal training

Mitigation During an Attack

As part of this package you will have access to customized 24/7 real-time alerting, specific to your site(s). This alerting helps identify anomalous traffic based on site-specific monitoring performed by Akamai systems. Should you suspect a DDoS attack, Akamai's Customer Care team is available 24x7 to help. They will, in coordination with your key stakeholders, declare that a malicious DDoS attack is occurring based on predefined thresholds and data analysis, and will execute defined procedures established in the SOP.

Deliverables:

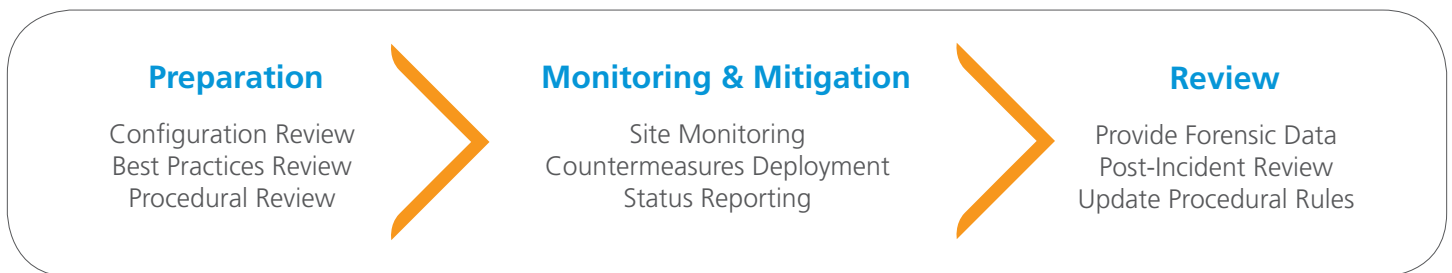
1. Assign named Akamai individual for Akamai DDoS incident coordination
2. Provide ongoing status updates until incident is properly mitigated
3. Implement additional mitigation measures and configuration changes as appropriate

Post-Incident Review

After an attack, Akamai Professional Services will update the SOP and Akamai service configurations, as needed. They will also provide your organization with data that enables you to conduct post-attack analysis, along with a report detailing the timeline of events, traffic graphs, observations, and recommended next steps.

Deliverables:

1. Integrate lessons learned into revised SOP
2. Provide data for forensic analysis
3. Provide an After Action Report for each DDoS incident
4. Revert back to normal business rules, as required



The Akamai Difference

Akamai® provides market-leading, cloud-based services for optimizing Web and mobile content and applications, online HD video, and secure eCommerce. Combining highly-distributed, energy-efficient computing with intelligent software, Akamai's global platform is transforming the cloud into a more viable place to inform, entertain, advertise, transact and collaborate. To learn how the world's leading enterprises are optimizing their business in the cloud, please visit www.akamai.com and follow @Akamai on Twitter.

Akamai Technologies, Inc.**U.S. Headquarters**

8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
(877.425.2624)

www.akamai.com

International Offices

Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore



©2010 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice.