Detection and responsiveness to
THWART DENIAL OF SERVICE ATTACKS

DoS Defense

Distributed Denial of Service (DDoS) attacks begin with a hacker exploiting multiple vulnerable computers on the Internet and utilizing these hosts to launch a coordinated attack on a target. The attack is aimed at overwhelming Internet-reachable resources within the target environment to a point where they are unable to perform their service function.

The volume and scale of DDoS attacks grow each year as threats become more numerous and blended in their composition and vector—the result of an increase of sophistication in both exploitation tools and their development. Powerful, readily available tools mean that criminals no longer need expert knowledge to commit an attack, enabling more people to act with malicious intent.

But the costs associated with remediating virus outbreaks and mitigating DDoS attacks can take a financial toll. And risk can never be completely eliminated. To safeguard business operations, risks must be prioritized and managed effectively—with comprehensive, scalable means.

Verizon’s DoS Defense service is a cloud-based DDoS protection service that gives you the ability to detect and divert potentially malicious DDoS traffic away from your network, helping you maintain the availability of Internet resources for legitimate users.

DETECTION AND MITIGATION

The service features the following fully scalable, proactive detection and mitigation capabilities:

• Network-based traffic analysis, anomaly detection, and alerts when your traffic patterns deviate from normal
• Performance and architecture suitable for enterprises large and small
• Alerts in the event of anomalous network detection that may characterize a virus or worm delivered via e-mail, SMS, or voice
• Automatic trouble-ticket generation when traffic anomalies are detected
• Automated health checks for Security Operations to ensure proper function and scale checks
• Secure web portal for access to reporting on security events, traffic patterns, applications, and configuration options

• Detailed reports showing graphical representations of packets, destination, and sources with downloadable feeds
• Audit trail, along with logged information and traffic files, to assist with law enforcement investigations, as necessary.

PROACTIVE DETECTION, RESPONSE, AND NOTIFICATION

Many DDoS attacks are the result of malicious worms and viruses prevalent in networks today. Proactive detection of these threats allows our engineers to mitigate attacks targeted at customer networks. And because DDoS attacks can be sourced from anywhere, we’ve shared these tools and techniques with other providers to create a higher level of awareness and overall responsibility within the Internet community.

DoS Defense enables our security engineers to proactively respond with notification and mitigation if you’re under attack. Along with proactive notification, you can view reports, open tickets, and obtain one-on-one security service. And it’s backed with a competitive service level agreement (SLA) covering:

• Configuration and activation
• Reactive response
• Administrative change
• Shared capacity

LEARN MORE

Our solutions combine security and infrastructure to help you secure data, identities, and your customers’ confidence from the desktop, along your network, and around the world. To learn more, contact your account manager or visit verizonenterprise.com/solutions/security.

verizonenterprise.com

© 2014 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon’s products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. FS11393 10/14