Advanced Rate Limiting

Summary

Signal Sciences rate limiting enables customers to protect their websites from abusive web requests with application-specific rate limiting rules that are easy to create. One-click actions enable further control over automated volumetric web requests.

Rate limiting protects against abusive behavior at the application layer that negatively impacts website and API performance. Attacks that Signal Sciences rate limiting protects customers against include:

- Brute force attacks
- Application/API denial of service
- Malicious high volume scripts
- Website content scraping
- API abuse
- Unintentional API overuse

Signal Sciences rate limiting stops excessive web requests from negatively impacting application and API performance by identifying and blocking requests that could result in abusive actions. Leveraging our award-winning app and API web protection technology, rate limiting provides intelligent controls to reduce the number of requests directed at key web application functions such as credit card validation forms, forgot password fields, email subscription sign-ups, gift card balance checkers and more.

Benefits of Rate Limiting

Stop application abuse with application-specific rules

Web requests that result in application abuse can blend in with legitimate traffic. Signal Sciences rate limiting is designed to identify such traffic and prevent individual IPs from causing app abuse.

Identify and stop requests from IP addresses that violate rate limiting rules

Quickly view real-time list of violators of rate limiting rules and then respond with easy one-click actions:

- Blacklist repeat violators
- Whitelist legitimate static IP addresses
- Remove rate-limited IP addresses as necessary

Rate Limiting Use Cases

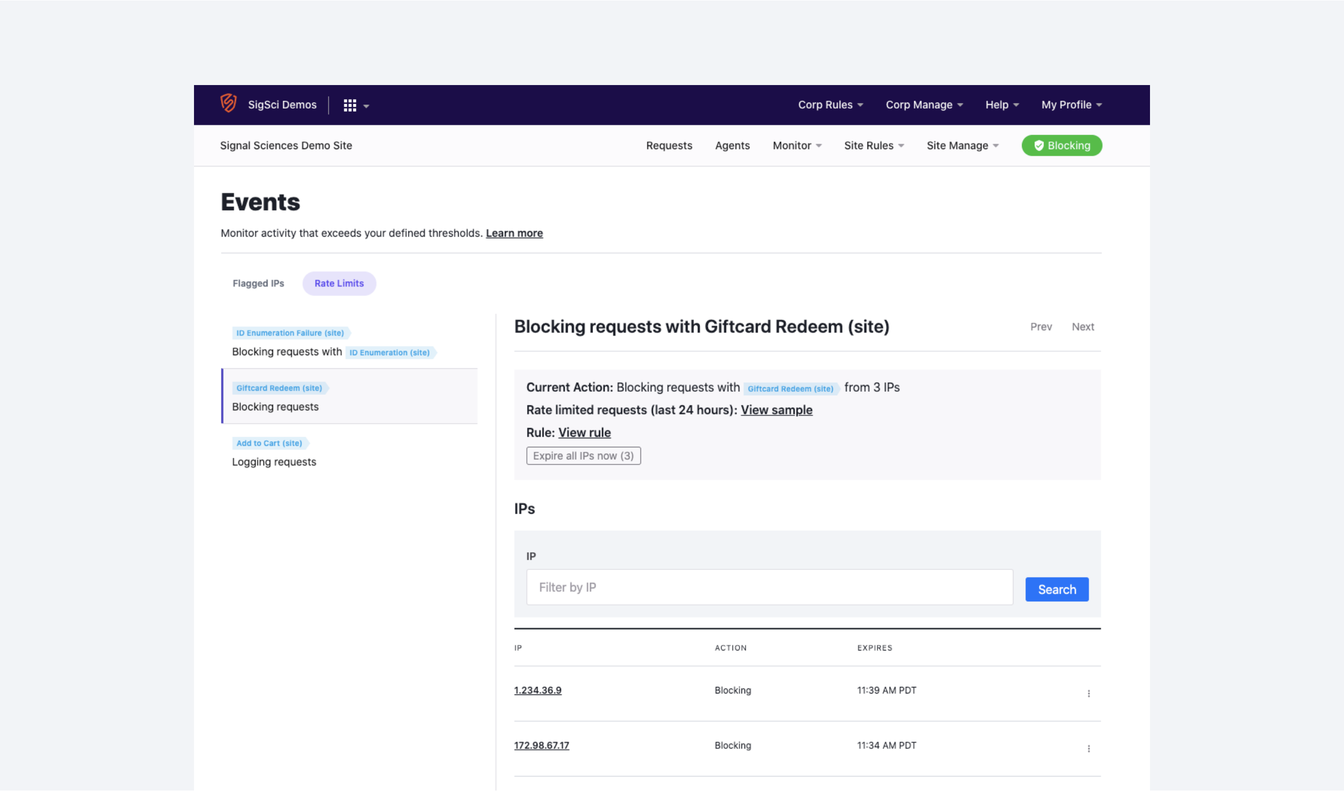
Use Case	Threat	Mitigation
Stop Excessive Views of Order Requests	Occurs when attackers direct too many requests at an ecommerce app's view order path in an attempt to enumerate order tokens.	• Stop high-volume requests to the view order path in a given timeframe • Block requests from known-bad IP addresses sending additional view order requests
Prevent Excessive 404 Responses	Attackers are sending too many requests resulting in 404 responses that overtax your app servers and use bandwidth that could be serving valid content or services to real customers.	• Block web requests from IPs sending too many requests that result in 404 responses during a given timeframe.
Block Excessive 'Add Credit Card' to Accounts	Cyber criminals use third-party websites to verify high volumes of stolen credit card accounts. Valid cards have not been cancelled and can be used to make purchases.	• Prevent any IP from sending too many requests attempting to add credit cards to accounts or verify credit card endpoints. • Block requests from IP addresses sending too many failed 'add credit card' requests. Failures can be identified via response code or response header.

Signal Sciences
Solution

Rate limiting from Signal Sciences stops malicious and anomalous high volume web requests and reduces web server and API utilization while allowing legitimate traffic through to your application and API endpoints.

Features

- **Easily setup application-specific rules to prevent app and API abuse**
- **Define custom conditions to block malicious requests**
- **Quickly identify and respond to a real-time list of IPs that have been rate limited**
- **Gain valuable insights into traffic targeting applications or API endpoints**
- **Reduce bandwidth costs by eliminating unpredictable traffic spikes and attacks**



Events

Monitor activity that exceeds your defined thresholds. Learn more

ID Enumeration Failure (site)
Blocking requests with ID Enumeration (site)

Giftcard Redeem (site)
Blocking requests

Add to Cart (site)
Logging requests

Blocking requests with Giftcard Redeem (site)

Current Action: Blocking requests with Giftcard Redeem (site) from 3 IPs
Rate limited requests (last 24 hours): View sample
Rule: View rule
Expire all IPs now (3)

IPs

IP
Filter by IP

IP	ACTION	EXPIRES
1.234.36.9	Blocking	11:39 AM PDT
172.98.67.17	Blocking	11:34 AM PDT

Signal Sciences makes it easy to create application-specific rate limiting rules. One-click actions enable further control over automated volumetric web requests.