What will you create?

With Section's edge compute platform, developers have the flexibility to choose the security solutions that best suit their application and make it easy to switch if/when necessary. In addition, Section has partnered with a growing list of leading security platforms, including Signal Sciences, ThreatX, PerimeterX, and Radware to offer a choice of next-generation web application security solutions.

Section

Web Application Security

Core Security Features

- **Network Layer DDoS Protection**
- **Traffic Overload Prevention/Virtual Waiting Room**
- **SSL/TLS Certificates and Management**
- **Visibility via Logs and Metrics**
- **IP Blocking**

Network Layer DDoS Protection

The Section platform is built on top-tier cloud hosting, so you'll get all the network layer protection and capacity provided by industry heavyweights like Microsoft and Amazon.

Traffic Overload Prevention / Virtual Waiting Room

This feature allows you to set a limit on the number of visitors who can reach your application at any one time and is also helpful in providing extra protection against DDoS or DoS attacks.

SSL / TLS Certificates and Management

Section provides all web applications with HTTPS automatically. If you don't have a SSL/TLS certificate, we will procure one for you and manage ongoing renewals so you don't have to.

Customers who want an extended validation certificate or who prefer to manage their security themselves can provide their own certificate at no extra cost. For customers with multiple domains, we can provide and manage SSL/TLS certificates for each domain.

Visibility via Logs and Metrics

Section provides ELK Stack logs and real-time metrics so you can inspect traffic easily within the Section portal, set up alerts and take immediate blocking action when needed.

IP Blocking

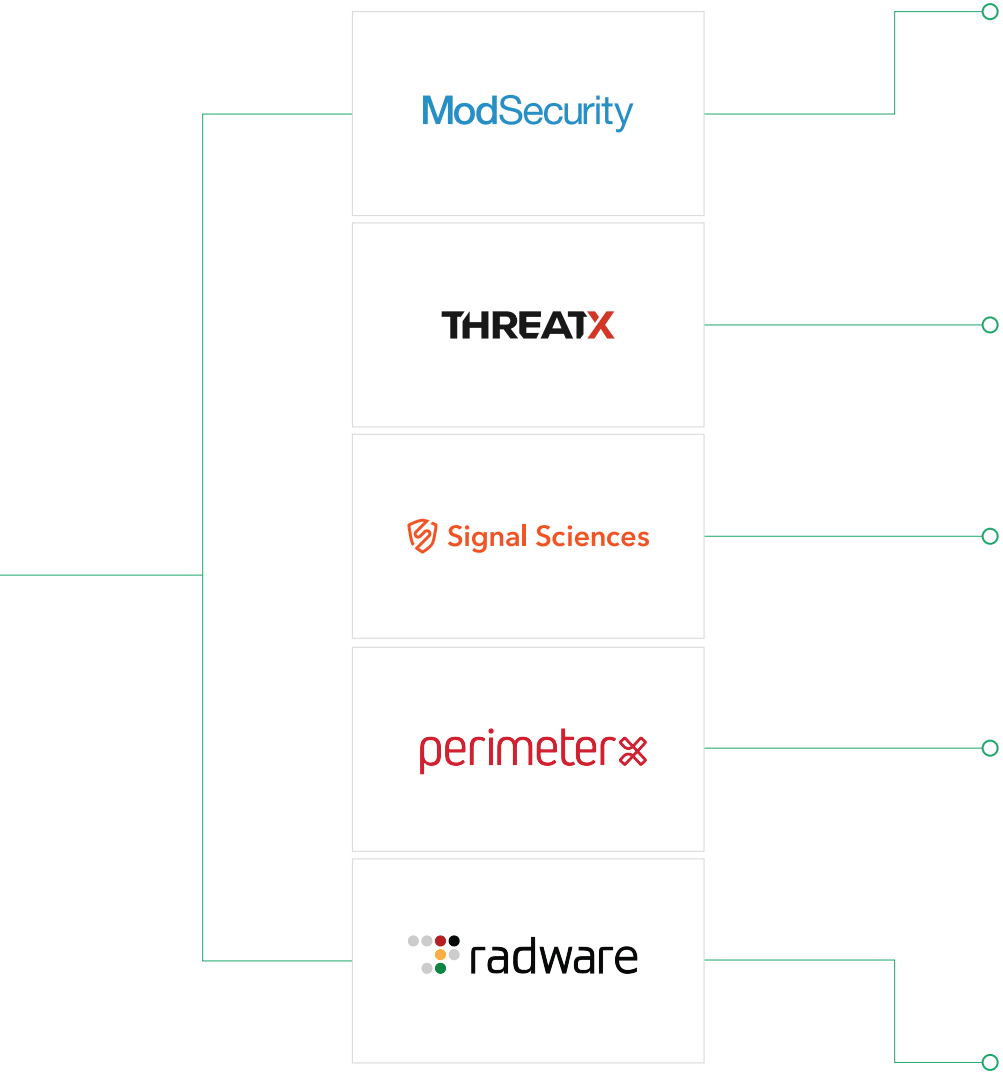
Quickly block specific IP addresses or ranges of IP addresses before they reach your origin server. This feature is useful in instances of malicious traffic from certain countries or suspicious activity from individual IP addresses.

GET IN TOUCH To discuss your specific needs or to get started with a free trial account, reach out to our experienced team of engineers:
info@section.io | US +1 844 325 9500 | AUS +61 2 9119 0444 | www.section.io

Section

Advanced Security Solutions

In addition to the core security features included, the Section platform also offers several advanced security solutions that are easily deployed and managed on our global network as edge container modules. This growing list includes the open source WAF ModSecurity, along with other industry-leading solutions from providers such as Signal Sciences, ThreatX, PerimeterX, and Radware. Each of these solutions give Section users greater control over their security and more advanced threat detection and blocking options.



ModSecurity - Open Source Web Application Firewall (WAF)

ModSecurity is a popular open source WAF that blocks threats via a set of rules. ModSecurity includes out-of-the-box protection against the Top 10 OWASP attacks and allows for unlimited custom rules. Section provides you with a fully configurable, unmodified version of ModSecurity with all the logs and metrics needed to quickly identify malicious activity.

ThreatX - Comprehensive WAF for Today's Hybrid Cloud

ThreatX is an intelligent WAF that learns your application's specific threat profile and automatically blocks threats while protecting legitimate traffic. ThreatX requires no configuration and is backed by a team of security experts who constantly monitor the latest hacker trends alongside your application's vulnerabilities. ThreatX factors out false-positives and escalates only when a specific entity has made progress to a level defined by you. Malicious traffic can be tracked, blocked, or slowed by redirecting it through a highly interactive network honeypot trap.

Signal Sciences - Next Generation Web Protection Platform

The Signal Sciences Web Protection Platform is an advanced security solution utilized by teams at Etsy, Vimeo, Under Armour and other high volume websites with enterprise-level security needs. Signal Sciences was created by CISOs, CTOs, and engineers looking to integrate advanced website security with cloud solutions and DevOps workflows.
The WPP analyzes and blocks threats in real-time, with 95% of customers using it in blocking mode, reducing false positives while identifying more threats than other solutions. Signal Sciences integrates with common tools including Slack, JIRA, and Kibana so you can get insights where you need them, when you need them.

PerimeterX - Security Solutions for Modern Applications

Leading enterprises trust PerimeterX to protect their websites and mobile applications from attacks aimed at stealing user data, personal information, and business critical content. Advanced behavioral analysis technology detects anomalies in user behavior including login dialogs and web-surfing patterns, preventing even the most sophisticated bot attacks. Solutions from PerimeterX help you discover risks, prevent attacks and act with confidence to win in the digital world.

Radware Bot Manager - Real-Time Bot Mitigation and Management

Radware Bot Manager specializes in delivering a best-of-breed, non-human traffic detection and management solution. Their advanced technology secures online businesses against automated threats such as content and price scraping, account takeover, gift card fraud, skewed analytics, ad fraud, and application DoS. Radware's bot detection engine utilizes multiple techniques to identify bots including proprietary Intent-based Deep Behavior Analysis (IDBA), user behavior analysis, device and browser fingerprinting, IP reputation, and machine learning.