Brochure

Lumen® DDoS Hyper® + Application Protection

A winning combination

LUMEN®
The Platform for Amazing Things℠

Overview

With cyberattacks on the rise, protecting your network, websites, applications, and APIs has never been more important. Lumen offers a holistic approach for web security that is designed to rise to the challenge of the modern threat landscape, all while supporting the changing business and technical needs of your company.

This document highlights the importance of protecting your web applications and APIs and reviews the benefits of pairing Lumen DDoS Hyper with Application Protection solutions.

LUMEN®

Lumen holistic web-protection

Digital economy and supporting applications and APIs are all going through generational transitions. To keep pace, security teams need a complete portfolio of cutting-edge solutions from the networking layer all the way up to the application layer that addresses today's challenges while also being able to quickly adapt to change.

Lumen provides a new approach to holistic application and API protection that helps solve the problems that have plagued traditional network security and application protection for years. With Lumen DDoS Hyper with Application Protection, companies can overcome challenges including fragmentation, duplicate solutions, inefficiency, inability to defend against new vectors of cyber-attacks, and more.

Lumen DDoS Hyper

DDoS attacks are becoming larger, more sophisticated and more strategic. If your business has critical web-facing assets, you could be a potential target for attackers.

To defend against the latest DDoS attacks, organizations need advanced detection and mitigation capabilities they can activate on their terms. Lumen DDoS Hyper provides multi-layer DDoS protection at your fingertips. With one of the largest DDoS mitigation deployments in the industry, backed by 170 Tbps of network-based mitigation capacity enacted at over 500+ multi-tiered scrubbing locations, Lumen owns DDoS mitigation at scale.

What sets Lumen DDoS Hyper apart from the competition?

1. **Spin up DDoS protection in minutes**

   A seamless and easy digital experience empowers you to get protection when you need it, even if you're under an active attack. Quote, buy and configure your solution in a matter of minutes, not hours.

2. **Advanced and feature-rich mitigation that fits your needs**

   Whether you're a Lumen internet customer or you bring your own network, DDoS Hyper can protect your infrastructure. Choose from monitoring and mitigation options that work best for you, such as Always-On or OnDemand and Flow-based monitoring.

3. **Keep budgets on track with predictable pricing**

   You don't control when you're going to be attacked, so why should you be punished? You'll get predictable flat rates with no usage charges no matter the size, frequency, or duration of DDoS attacks.

> "Lumen provides its customers with state-of-the-art products and services that enable secure application experiences. The company's Holistic Web Protection solution streamlines enterprise customers' web application security. It also complements other features of the Lumen Platform designed to support customers on their digital transformation journey."
>
> -- Steven Lopez
> Best Practices Research Analyst, Frost & Sullivan

DDoS Hyper Features & Specs

- Quote, order and configure online through Lumen Marketplace
- On-Demand and Always-On mitigation available
- Flow-Based monitoring included
- Network-based unlimited mitigation
- Global multi-tiered scrubbing architecture
- Carrier-agnostic defense with GRE clean traffic return or Lumen network customers can take advantage of Internet Direct.
- Proactive monitoring and alerting from global SOCs
- 1-second time-to-mitigate once traffic hits the scrubbing centers
- Predictable monthly or annual contracts
- Clean traffic return options up to 100 Gbps
- SOC assisted services hours available for additional purchase
- Automated blocking and defense fueled by Black Lotus Labs® threat intelligence

“**170 Tbps** of network-based mitigation capacity across 500+ global scrubbing locations.”

API and Application Protection

As web applications and APIs continue to evolve and expand in microservice dominated environments, application layer cyber threats become more sophisticated, diversified, and complex, requiring a new generation of application security solutions. Lumen® Application Protection offers an innovative approach and a new generation of application security solutions, by combining Artificial Intelligence (AI), Machine Learning (ML) powered cyberattack detection, attacker-centric behavior analysis, real-time blocking against complex multi-mode attacks, and the ease of cloud-native deployments all supported by a dedicated team of AppSec experts.

- **Web Application Firewall**

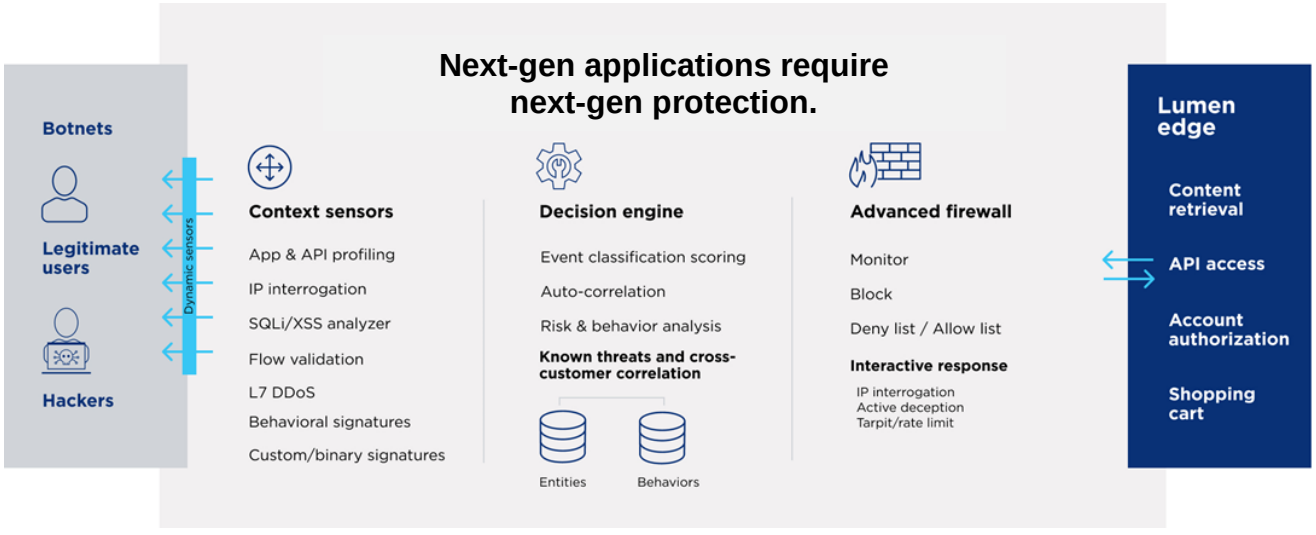
  Web Application Firewall (WAF) learns an application's specific threat profile, and automatically blocks threats, while protecting legitimate traffic. While traditional WAFs had to be tuned to handle threats, this has caused many companies to be reactive instead of proactive. With Next-Gen WAFs provided by Lumen, companies can simply deploy a WAF, which evolves on its own with the threats that it encounters. This solution provides peace of mind for companies who deal with online services, and allows developers to spend their time working on other projects.

- **API Protection**

  APIs are a critical part of conducting business online, as they enable DevOps teams to quickly deliver products/services, which help grow and evolve their business. However, they are under immense pressure from cyber-attacks. Lumen provides an API Attack Protection platform that stops API attacks in real-time. Through Lumen Application Protection, customers can: Detect and block attacks, enable advanced forensics, discover and defend APIs, visualize API attack surface, and enforce API schema compliance.

- **Bot Risk Management**

  There are good bots that help customers find the best coupons on an item or find flights at the lowest cost. Then there are bad bots who preform malicious acts such as credential stuffing and content scraping. Bot Risk Management (BRM) is a solution Lumen provides designed to prevent these bots from ever attacking.



What makes Lumen different from other API & Web Application Protection Solutions?

1. **Single risk engine/multi-layered detection capabilities**

   While other solutions provide single attack visibility, Lumen's multi-layered detection capabilities process Edge, Bot, and API activity via a single risk engine, automatically correlating this data to provide a full view of the activity and potential risk.

2. **Attacker behavioral analytics**

   Unlike traditional security solutions that rely solely on signatures and static rules, Lumen leverages an attacker behavioral-based approach to accurately identify malicious actors by building dynamic profiles on each threat entity as they move through the kill-chain, despite the multiple tactics or duration of the attacker's campaign, and take appropriate action, including blocking the threat if necessary. Customers can also apply proprietary signature-based rules.

   This, combined with the multi-mode detection approach designed to significantly improve threat visibility and blocking efficacy while reducing business disruption, tuning, rule-writing, and operational overhead.

3. **Ease of deployment/time-to-value**

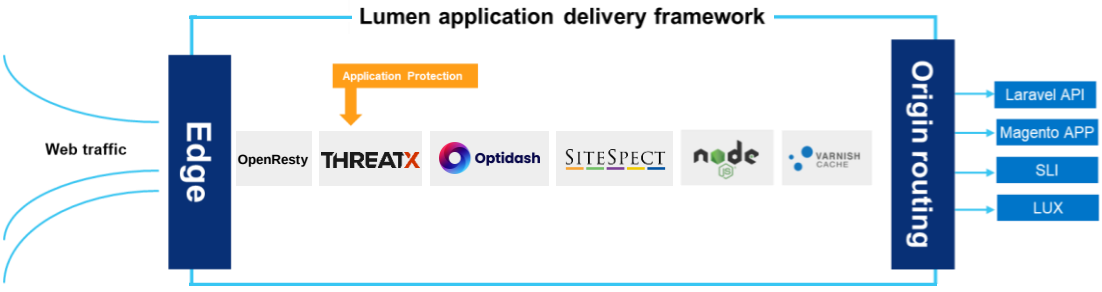
   Teams can typically deploy Lumen Application Protection within 30-minutes and be in full blocking mode within 72 hours. Application Protection can be deployed on several major cloud providers, on premises, or hybrid deployments.

   Lumen's deployment model allows for teams to quickly get up and running and easily scale across additional APIs and Web Apps to securely support the demands of the business

4. **24/7 Managed SOC**

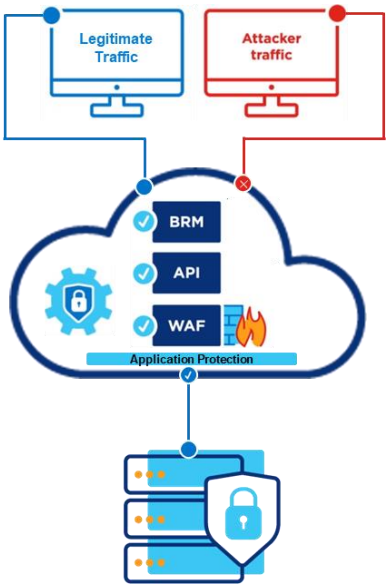
   Lumen Application Protection is delivered via 24/7 managed SOC staffed with API and web apps experts

   Working as an extension of the customer's team, Lumen SOC will perform daily administration of the platform, ops monitoring, IR, threat hunting, and custom countermeasure development



Simply add any of our best-in-breed Application Protection modules onto your DevOps workflow for seamless API and Application Protection.

Application Protection Features & Specs



- Real-time detection & blocking
- Application Profiling: Machine learning determines appropriate application inputs and responses while adapting to application and environmental changes to enable better baselining, faster threat identification, and fewer false positives
- Full control over WAF service management and configurations
- Web application protection from threats across cloud, premises, and hybrid environments
- Combination of behavior profiling, threat intelligence and analytics to identify suspicious behaviors and associated risks
- Shared threat analytics correlate attack patterns and techniques across multiple customers and applications
- Support for a virtual version of the environment to rapidly test new code and capabilities

> “As a small and specialized team, we don’t have the ability to just watch out for potential threats or suspicious activity. Using ThreatX on Lumen has been a game changer for my team and me and has provided an additional layer of security for our members.”
>
> -- Director of IT

Why Lumen?

Lumen DDoS Hyper and Application protection are a winning combination. We provide the security essentials by offering a unified and easy-to-use experience where customers can integrate and customize the best-of-breed vendors to protect their web-facing assets.