BROCHURE

Accelerating and securing the digital experience

LUMEN℠

It’s time to break the monolith

In today’s digital economy, the underlying applications and workflows that power organizations must be agile, secure and perform in an optimal manner. As workloads and data move closer to end users, development teams battle monolithic infrastructures that are inflexible and unable to scale – slowing down innovation, constricting development cycles and reducing application security and performance.

Today’s DevOps teams must be empowered to easily configure, stage and push changes into production quickly without taking environments offline, diminishing user experience or making web applications vulnerable to threats. Combined with the increasing frequency and sophistication of targeted network and application layer attacks, organizations need advanced detection, analysis and rapid response to threats and malicious behaviors that can put mission-critical workloads and user experience at risk.

One of the biggest challenges facing organizations today is how to overcome the constraints of a monolithic infrastructure and move to an agile environment that both accelerates and secures digital interactions.

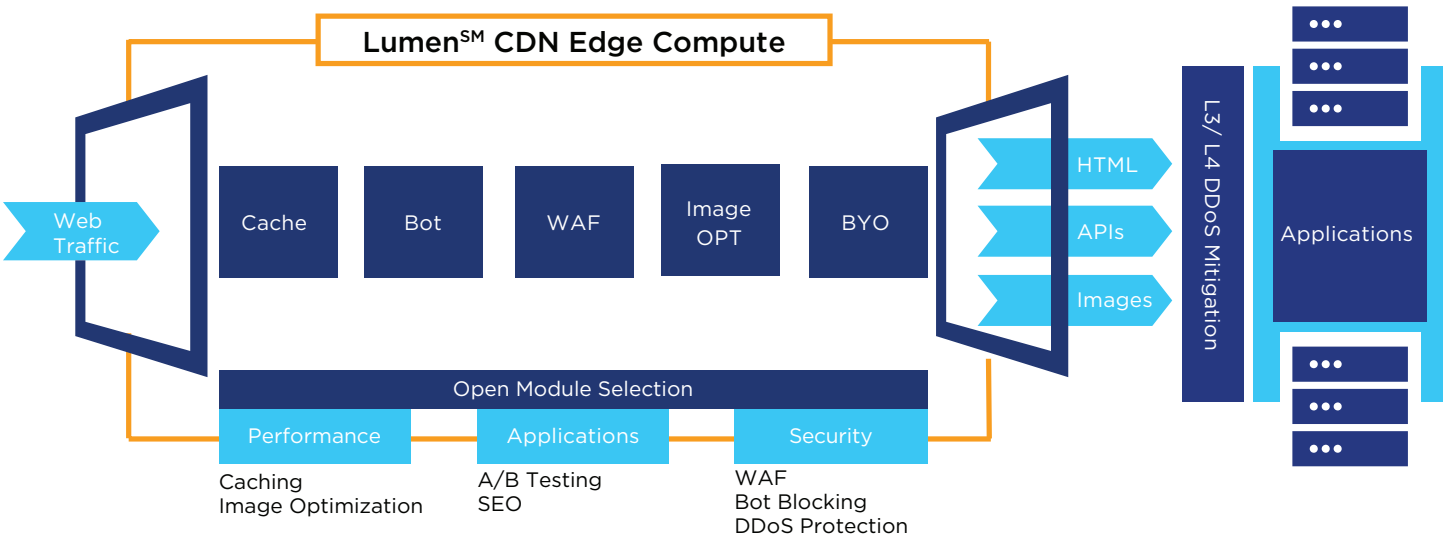
What’s in your container?

Breaking the monolith means organizations must rearchitect their application environments to better enable new generation digital experiences. This posture is achieved by leveraging the latest advancements in containerized workloads.

Lumen's container-based deployments are infrastructure agnostic, allowing applications and security policies to be broken into microservices that can be orchestrated and auto-scaled across a wide geographic area. Therefore, businesses no longer need to focus on resourcing compute and storage requirements as containers isolate the application from the underlying technology infrastructure. Organizations can tailor their containers and security policies to individual workloads and workflows to better enable end-user digital interactions while securing the application experience at the edge.

With the secure Lumen CDN Edge Compute platform, enterprises can accelerate development workflows, optimize performance and secure applications through containerized modules designed to power digital interactions.

Our container-based platform empowers DevOps with self-service, software-defined control to run workloads with processing closer to end users for optimal application performance. Additionally, Lumen CDN Edge Compute enhances performance using Varnish Dynamic Caching, image optimization and static caching technologies. Supporting greater flexibility and increased speed-to-market, Lumen's platform enables a digital twin to be easily created, allowing developers to stage and test new configurations so changes can be pushed into production quickly for rapid time to value.



Through the Lumen CDN Edge Compute platform, businesses can "bring your own software" or choose from a marketplace of best-in-breed edge security software solutions to tailor defenses for web applications – while avoiding vendor or technology lock-in. These next-gen controls can be swapped out real-time to give enterprises more flexibility and control over their security postures.

Additionally, these containerized environments can be service-chained to build out a multilayered security policy, giving organizations the flexibility to customize security stacks across best-in-breed WAF, bot management and API protection solutions offered in the Lumen CDN Edge Compute marketplace. These containers can be orchestrated across our global network edge to create an environment that is agile and flexible, all while delivering security policies tailored to the customer's individual workflow or workload.

Lumen's open module marketplace

Disrupting the disruptors

Helping combat disparate point solutions and inflexible edge software, the Lumen CDN Edge Compute platform strengthens Lumen's robust portfolio of global DDoS mitigation solutions to help provide full-spectrum, layer 3/4 and layer 7 application defenses and acceleration for customers. And with large-scale volumetric attacks designed to disrupt mission critical applications and services, organizations need access to Lumen's significant ingest capacity and advanced scrubbing capabilities to keep up.

Defense in-depth DDoS mitigation

Lumen has one of the largest global DDoS mitigation deployments in the industry. Because of Lumen's highly distributed network edge and deep peering, customer applications benefit from improved performance and attack detection and mitigation occurring on the Lumen backbone.

Lumen mitigates ~120 DDoS attacks daily

~89% of the top 100 DDoS attacks were multi-vector

~19% of top 100 DDoS attacks targeted the application layer

Even attacks that can't be blocked with application layer controls, like bandwidth intensive volumetric DDoS traffic, can be absorbed by CLumen's ~85+ Tbps of global backbone FlowSpec capacity and/or dropped at the network edge and directed to scrubbing centers only when needed, improving scale and performance. By shifting the first line of defense upstream, the Lumen network can detect and block malicious activity before it impacts customer environments or consumes resources connecting to that environment.

As a second line of defense, Lumen has deployed a multi-tiered global scrubbing infrastructure to support DDoS attack mitigation within the network. Lumen's three-tier scrubbing architecture is designed to minimize network latency and the impact of multiple large-scale attacks operating at the same time, whether directed at an organization's web-facing sites and applications or another Lumen customer being served within our local and regional centers. Very large attacks are automatically and intelligently routed to super scrubbing centers when thresholds are exceeded, thereby reducing the potential for collateral damage when others experience significant volumetric attacks.

Intelligent routing and attack mitigation

The First Tier

is comprised of local scrubbing centers whose purpose is to minimize latency in market as Lumen triages attack traffic. The network architecture is designed in such a way that an attack will start to be mitigated within the local scrubbing center. Depending on the size of the attack, this can be elevated up to regional scrubbing centers and ultimately supported via the super scrubbing centers as needed.

The Second Tier

is comprised of regional scrubbing centers. These sit within the major geographic regions and deal with larger attacks originating within that region.

The Third Tier

is comprised of super scrubbing centers close to large concentrations of internet traffic; we use these to “ring fence” significant attacks, making sure there’s no cascade effect to any other customers that may also be under mitigation.

1: Local scrubbing centers

- Minimize latency
- Reduce collateral impact

2: Regional scrubbing centers

- Deal with larger attacks originating within the regions

3: Super scrubbing centers

- Handle super large attacks
- Close to major internet traffic peering points

This architecture provides clear advantages for Lumen℠ DDoS customers by ensuring that the increase in latency, while under mitigation, is minimized. It also provides protection from the impact of other customers’ traffic – the tsunami effect where multiple customers are under attack in the same region.

Are you ready to break the monolith?

- A DevOps-friendly edge compute platform that accelerates application performance to enhance digital interactions globally
- The ability to support the creation of a digital twin for rapid testing and deployment
- A modular marketplace of next-gen WAF, bot management and API protection solutions delivered through Lumen CDN Edge Compute platform containers
- An environment where containers run within milliseconds of end-users, reducing cost and bandwidth constraints between origin servers to enhance application performance
- A simplified experience where customers can rapidly orchestrate and deploy security controls targeted to individual workflows in near realtime development cycles
- A global, robust network-based DDoS solution facilitated by one of the world's largest and most deeply peered IP backbones to support end-to-end layer 3/4 and layer 7 protection

Don't wait for an inflexible tech stack to play catch up. Let Lumen help you break the monolith.

Footnotes

1. According to Gartner, "by 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications.

877-453-8353 | lumen.com

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2020 Lumen Technologies. All Rights Reserved.

LUMEN℠