

Scalefusion Increased Platform Resilience

SaaS security platform improved uptime and blocked millions of attacks with App & API Protector



Blocked 515M attacks in 90 days



Strengthened platform availability



Improved user experience

Helping IT and security teams work as one

Scalefusion, built by [ProMobi Technologies Pvt Ltd.](#), is a platform helping companies manage and secure devices, users, and access from a single console. This SaaS suite supports more than 12,000 customers and millions of endpoints across healthcare, banking, logistics, retail, and education.

As remote work surged during COVID, Scalefusion saw traffic rise fast. That growth increased security risks and put more pressure on platform uptime. To protect its public-facing applications and [APIs](#), the company replaced its existing provider with Akamai App & API Protector. The move improved resilience and reduced latency. It also gave Scalefusion stronger control over security at scale.

Managing fast growth and rising risk

The Scalefusion suite enables unified endpoint management, [endpoint security](#), and [Zero Trust](#) access. “We help IT and SecOps converge into a single pane of glass,” said Vivek Lokhande, Director of DevOps and Compliance at Scalefusion. “That reduces tool fatigue and helps IT and security teams work better.”

Traffic to Scalefusion’s platform grew quickly during the COVID years as more employees used personal devices and worked outside traditional networks. The company currently manages around 10 million devices, with 7 million active at any time. Those devices send [constant requests](#) back to the platform.

That scale brought new challenges. “There are two ways someone can access your network,” said Lokhande. “The internal side is under our control. The internet is not.”

Scalefusion needed stronger protection at the [edge](#).

Its earlier WAF provider struggled under attack. During [DDoS](#) events, Scalefusion’s team often had to step in and make manual changes to keep services running.

“Sometimes we had to throttle traffic to protect our infrastructure,” Lokhande continued.

That slowed services and hurt the user experience.



Location

Pune, India

scalefusion.com

Industry

[Software and SaaS](#)

Solution

[Security](#)

Product

[App & API Protector](#)



Finding the right web application firewall for scale

Scalefusion explored several options, including open source tools and other leading providers in the market. But most of the available pricing models weren't workable. Scalefusion handles about 30 million **HTTP** requests each day. Since several providers charge by request count, costs would have climbed quickly.

Akamai **App & API Protector** offered a different approach. "Akamai gave us throughput-based pricing," said Lokhande. "That worked better for our traffic."

That model suited Scalefusion because most of its traffic is lightweight device check-ins. The devices often send simple "I am alive" messages instead of large data payloads.

Akamai also stood out for its reputation in security. That trust mattered to Scalefusion as it looked for a long-term partner.

Testing fast and moving quickly

Scalefusion ran a one-month proof of concept of App & API Protector. The team explored the control center, tested policies, and reviewed how the platform handled traffic.

"We tested how App & API Protector worked and saw it would fit our environment," explained Lokhande.

The team liked how Akamai handled testing and rollout. It could build and test in staging before pushing changes live. "The versioning and rollback features impressed us, as they reduce risk," he continued.

Scalefusion also wanted the solution to be adaptive, offering AI/ML-based recommendations. "Akamai provides that, helping us improve our security analysis efforts. This affirmed our decision to choose Akamai," he added.

After four weeks of testing, Scalefusion moved into production.

Strengthening API and application security

Today, App & API Protector secures all of Scalefusion's public-facing applications and APIs. The company uses the solution to stop attacks, filter traffic, and keep services online.

App & API Protector includes:

- **WAF:** Protects web apps from common threats and exploits
- **API protection:** Detects risky API behavior and blocks abuse
- **DDoS protection:** Stops attacks before they impact services
- **Bot defense:** Filters harmful automated traffic
- **AI-driven adaptive tuning:** Recommends best rule settings based on traffic patterns

"We didn't have to do anything once we set rules in App & API Protector," said Lokhande. "It applies them very well and continuously adapts."

Akamai also improved certificate management. Through Akamai's **DigiCert** integration, Scalefusion now handles renewals more easily. "We don't have to think about certificate renewals anymore," he added.



Akamai gives us complete peace of mind. We haven't experienced a single service-impacting security event in three years.

Vivek Lokhande
Director of DevOps and
Compliance, Scalefusion

Blocking attacks at massive scale and gaining better visibility

The numbers show the scale of protection. In 90 days, Scalefusion clocked 34 billion hits across its infrastructure. Out of those, Akamai blocked 515 million attacks. That includes DDoS traffic, scraping attempts, and other malicious requests.

Scalefusion can see how many attacks Akamai blocks over time. “That visibility helps us understand trends and act faster when needed. It also helps prove the value of our security investments,” Lokhande said.

Scalefusion feeds Akamai logs into its own SIEM (security information and event management) and observability systems. That gives the support team a clearer view when customers report issues. The company also built its own AI-driven Model Context Protocol (MCP) platform to correlate logs, accelerating root cause analysis.

“If a customer has an issue, we combine Akamai logs with our own logs and find the problem quickly,” said Lokhande.

Improving uptime and customer confidence

Availability is critical for the Scalefusion platform. The company promises 99.95% uptime to its customers.

Before Akamai, attacks made that harder to maintain. Today, the team feels much more confident. “We are more resilient now,” said Lokhande. “Our security team can focus on improving Scalefusion instead of reacting during an attack.”

In fact, Scalefusion has not had a single service-impacting DDoS event in the past three years. As a result, users have a better user experience, and the company has boosted its market standing and brand credibility.

That impact has changed how Lokhande feels about his job. Before Akamai, the stress was constant. “Sometimes we felt helpless,” Lokhande said. “We were doing our best, but some attack vectors were too strong. I sleep well now,” he continued.

Supporting growth with confidence

The Scalefusion platform runs across AWS, DigitalOcean, Azure, and Google Cloud. This multicloud model gives the company flexibility as it grows.

Akamai fits into that strategy as the main protection layer for internet traffic. “We want to avoid dependence on one cloud provider, especially as we expand into new markets,” Lokhande explained.

Akamai has also helped Scalefusion win customer trust. Many enterprise buyers, especially in banking, already know and trust Akamai. That recognition helps during the sales process. “When customers see that we use Akamai, it gives them confidence,” he continued.

“We are able to retain existing customers and sign new ones because of Akamai,” Lokhande concluded.



Scalefusion provides a comprehensive suite of products engineered to simplify endpoint, user, and access management for IT teams. The powerful product lineup includes Scalefusion UEM for streamlined device management, Scalefusion OnIdP for secure zero-trust access, and Scalefusion Veltar for advanced endpoint security. With over 12,000+ businesses in 120+ countries trusting our products, Scalefusion ensures your business is always one step ahead.