

imperva

THALES
CYBERSECURITY

Why Organisations are Switching to Imperva Network DDoS

Modern DDoS attacks are faster, larger, and more complex than ever. When mitigation depends on manual tuning, separate consoles and long response windows, downtime becomes a real business risk. Organisations often outgrow legacy DDoS providers where response depends on manual intervention, rule changes and lengthy services engagements. Imperva Network DDoS helps teams move faster and delivers automated mitigation designed to stop attacks before they impact availability.

What makes Imperva different?

Imperva combines network, transport, and application-layer DDoS protection in a single platform with unified management across WAF, Bot Management and API Security. Organisations can replace slow, service-heavy DDoS response with a simpler approach that reduces operational burden, shortens deployment timelines, and lowers total cost of ownership.

	Imperva Network DDoS	Akamai Prolexic
What happens during an attack?	Attacks mitigated automatically before impact with no action required	Variable mitigation speed due to attack type and rule coverage — risk of impact during response window
Mitigation approach	Fully automated, intelligent mitigation on a single platform	Service-led, manual tuning and adjustments
Attack readiness	Continuously validates and displays attack readiness through tunnel health monitoring, network advertisement verification, traffic path validation, and expected traffic level checks.	Does not validate that traffic is actively traversing the intended mitigation path. Routing changes or configuration drift may result in traffic bypassing mitigation infrastructure without visibility into the issue.
Multi-vector attack protection	Built-in protection across network, transport and application layers	May require separate handling across layers
Operational complexity	Single platform, unified console — DDoS, WAF, Bot, and API Security managed in one place	Separate DDoS platform and management console — distinct from WAF, Bot, and API Security
Engineering lift	Designed to be deployed and managed without a large services engagement	Heavy services wrap for setup, configuring and live attack handling
Replacement or rollout deployment time	Typically days to full protection	May be extensive due to service complexity and operational overhead
Cost model	Lower TCO with simplified operations and no hidden fees. Global subscription provides greater flexibility for customers that need to scale protection across multiple locations.	Per-location pricing model results in higher cost with hidden service and operational overhead.
Mitigation SLA	Committed sub-3-second time to mitigation with a guaranteed response. Unconditional guarantee with no SOC collaboration required. Customers connecting each of their data centers to three Imperva PoPs (Points of Presence) are eligible for an enhanced uptime SLA of 100%. Maintains the same sub-3-second mitigation commitment even as attacks evolve or shift across vectors.	0-second SLAs apply only to preconfigured SOC rules. Novel DDoS attack vectors may require 5–10 minutes to mitigate under Akamai's SLA, depending on the attack type. For morphing or multi-vector attacks, each newly introduced attack vector may require a separate mitigation cycle, potentially resulting in repeated 5–10-minute impact windows as the attack evolves.
Ongoing management	Minimal ongoing management required	Continuous tuning, service dependency, complex configuration and expertise needed
Beyond Network DDoS	Single platform extends natively from Network DDoS to WAF, Bot Management, and API Security — one contract, one console, one security stack	Network DDoS protection, WAF and L7 DDoS, advanced bot, and API security are distinct platforms, each with separate licensing, and integration requirement

"Imperva Network DDoS gives us the scale and automation we need to stay ahead of volumetric attacks. It's one less thing we have to worry about—and that peace of mind is huge."

"We actually did get a volumetric attack that flipped over at like, 4:00 in the morning, and we automatically flipped the network that was being attacked over to Imperva. I was able to log in and see that it was a 300-plus gigabit per second attack that would have taken down our entire network."

Gabriel Mangieri, CTO at Fusion Networks

Read the full case study

"I had a great overall experience with Imperva DDoS Protection. It is dependable, quick and successfully maintains services online even in the face of frequent attacks"

IT Services Organisation

Read Gartner Peer Insights Reviews

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Ready to see how quickly you could replace or complement your current DDoS provider?

Book a demo or speak with an expert to review your current architecture and attack readiness.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

© Thales - September 2026 • HP . v7