The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021

The 11 Providers That Matter Most And How They Stack Up

by David Holmes
March 3, 2021

Why Read This Report

In our 28-criterion evaluation of DDoS mitigation solution providers, we identified the 11 most significant ones — A10 Networks, Akamai Technologies, Alibaba Cloud, Amazon Web Services, Cloudflare, Google, Imperva, Lumen, Microsoft, Neustar, and Radware — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

Cloudflare, Radware, Akamai Technologies, And Imperva Lead The Pack

Forrester's research uncovered a market in which Cloudflare, Radware, Akamai Technologies, and Imperva are Leaders; Amazon Web Services and A10 Networks are Strong Performers; and Google, Microsoft, Alibaba Cloud, Neustar, and Lumen are Contenders.

Cloud Asset Protection, Layer 7, And Response Automation Are Key Differentiators

As the on-premises DDoS protection approach becomes outdated, improved cloud delivery and service will dictate which providers will lead the pack. Vendors that can deflect both enormous floods and sneaky layer 7 attacks position themselves to successfully deliver origin and cloud asset protection as a service to their customers.

FOR SECURITY & RISK PROFESSIONALS

The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021

The 11 Providers That Matter Most And How They Stack Up

by David Holmes
with Joseph Blankenship, Alexis Bouffard, and Peggy Dostie
March 3, 2021

Table Of Contents

Related Research Documents

The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020

Now Tech: DDoS Mitigation Solutions, Q2 2020

Remove The Mystery From Security Metrics

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

The Old Guard Excel, But The Cloud Providers Are Catching Up Fast

Here's the thing: DDoS attacks themselves haven't changed that much since Forrester's last DDoS protection Forrester Wave™ in 2017.[1] The DDoS protection market, however, certainly has. There are three major trends in the DDoS protection market. First, 75% of surveyed global security decision-makers want to consume DDoS protection as a service instead of racking hardware themselves.[2] Second, applications have continued their migration out of the private data center and into the cloud, shrinking the market for on-premises DDoS solutions largely to those that provide it as a service. And last, but most significantly, in 2017 most public cloud service providers (CSPs) didn't offer DDoS mitigation services for general availability, but now they all do.[3]

As a result of these trends, DDoS protection customers should look for providers that:

- **Protect cloud assets.** Every application owner and developer moving their application to a public CSP will, of course, be interested to see how well that CSP is positioned to protect their applications. Leveraging the CSP's DDoS protection infrastructure seems like a no-brainer; the CSP is already trusted with the application, the data, and its availability.

- **Can defend layer 7 without a WAF.** Determined attackers can make life messy at layer 7 with heavy queries or malformed requests. For years, the "solution" offered by the market was to use a web application firewall (or WAF). But not all assets are web applications, and WAFs require far more maintenance than DDoS protection. WAFs are also incompatible with the on-demand model.

- **Automate not just detection but response.** Let's face it; the internet is a toxic wasteland of malicious automation. Ask anyone who has ever stood up a public-facing SSH server how long it takes for brute force attacks to appear in their logs (spoiler: it's often less than a minute). DDoS is the original malicious automation, and attackers leverage it all day long. To keep the most malicious automation attacks from overloading your own humans, look for providers that can automate all mitigations, even the zero-day DDoS attacks that occur every year.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our "Now Tech: DDoS Mitigation Solutions, Q2 2020."

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: DDoS Mitigation Solutions, Q1 2021

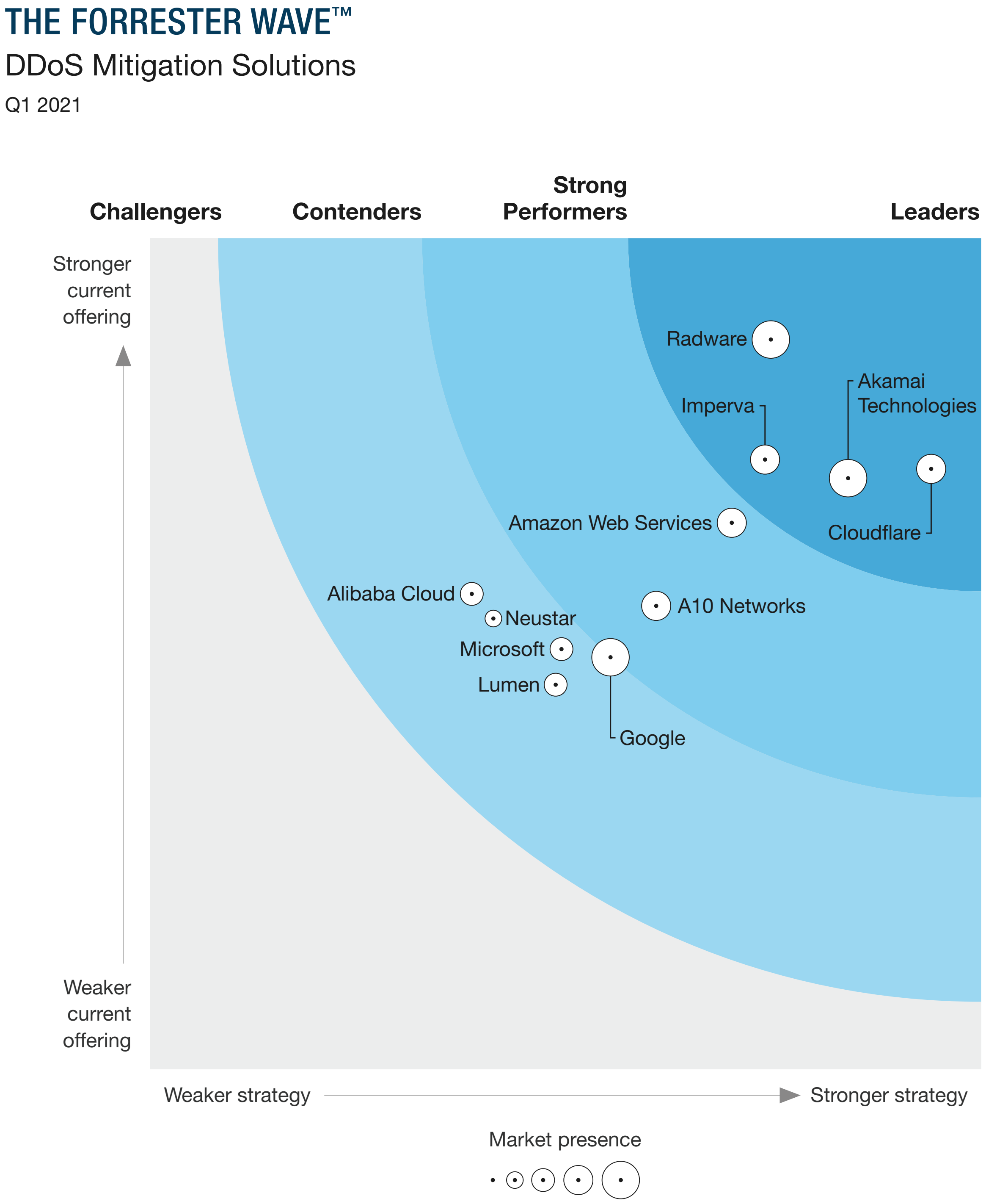

FIGURE 2 Forrester Wave™: DDoS Mitigation Solutions Scorecard, Q1 2021

	Forrester's weighting	A10 Networks	Akamai Technologies	Alibaba Cloud	Amazon Web Services	Cloudflare	Google
Current offering	50%	2.79	3.56	2.86	3.29	3.61	2.48
Volumetric scrubbing	15%	1.00	5.00	2.40	5.00	4.20	3.80
Public cloud asset protection	10%	3.00	1.00	3.00	5.00	3.00	5.00
Detection and attack mitigation	20%	4.44	3.28	3.00	2.72	4.16	1.56
Security operations centers	5%	3.00	5.00	1.00	3.00	5.00	3.00
Response automation	10%	5.00	3.00	5.00	3.00	5.00	1.00
Speed of implementation	5%	1.00	3.00	5.00	5.00	5.00	3.00
Alerting	5%	3.00	3.00	5.00	3.00	3.00	3.00
Regulatory compliance	5%	1.00	3.00	3.00	5.00	1.00	3.00
Service delivery	5%	3.00	5.00	3.00	1.00	3.00	3.00
On-premises component	5%	5.00	1.00	0.00	0.00	1.00	0.00
Service agreements	10%	0.00	5.00	1.00	3.00	3.00	1.00
Threat intelligence	5%	3.00	5.00	3.00	1.00	3.00	3.00
Strategy	50%	3.05	4.20	1.94	3.50	4.70	2.77
Product vision	12%	1.00	3.00	1.00	3.00	5.00	3.00
Planned enhancements	28%	5.00	3.00	3.00	3.00	5.00	1.00
Performance	10%	5.00	5.00	3.00	5.00	5.00	5.00
Pricing model	15%	1.00	5.00	1.00	5.00	3.00	5.00
Development and support	35%	2.50	5.00	1.50	3.00	5.00	2.50
Market presence	0%	4.00	4.50	2.25	3.75	3.50	4.25
Current revenue	75%	5.00	5.00	2.00	4.00	3.00	4.00
Installed base	25%	1.00	3.00	3.00	3.00	5.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 2 Forrester Wave™: DDoS Mitigation Solutions Scorecard, Q1 2021 (Cont.)

	Forrester's weighting	Imperva	Lumen	Microsoft	Neustar	Radware
Current offering	50%	3.67	2.31	2.53	2.71	4.39
Volumetric scrubbing	15%	2.20	2.80	2.40	3.80	3.60
Public cloud asset protection	10%	3.00	1.00	5.00	1.00	5.00
Detection and attack mitigation	20%	4.44	2.72	1.84	2.96	5.00
Security operations centers	5%	3.00	3.00	1.00	3.00	5.00
Response automation	10%	3.00	1.00	1.00	0.00	5.00
Speed of implementation	5%	5.00	3.00	5.00	3.00	1.00
Alerting	5%	5.00	1.00	3.00	3.00	3.00
Regulatory compliance	5%	3.00	1.00	5.00	1.00	5.00
Service delivery	5%	5.00	1.00	1.00	5.00	5.00
On-premises component	5%	1.00	3.00	0.00	3.00	5.00
Service agreements	10%	5.00	3.00	3.00	5.00	5.00
Threat intelligence	5%	5.00	5.00	3.00	1.00	3.00
Strategy	50%	3.70	2.44	2.48	2.07	3.74
Product vision	12%	5.00	3.00	1.00	3.00	3.00
Planned enhancements	28%	5.00	1.00	1.00	1.00	5.00
Performance	10%	5.00	3.00	1.00	1.00	3.00
Pricing model	15%	1.00	3.00	5.00	3.00	3.00
Development and support	35%	3.00	3.00	3.50	2.50	3.50
Market presence	0%	3.25	2.75	3.00	2.00	4.25
Current revenue	75%	3.00	3.00	3.00	2.00	4.00
Installed base	25%	4.00	2.00	3.00	2.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Vendor Offerings

Forrester included 11 vendors in this assessment: A10 Networks, Akamai Technologies, Alibaba Cloud, Amazon Web Services, Cloudflare, Google, Imperva, Lumen, Microsoft, Neustar, and Radware (see Figure 3). We invited F5 Networks, Huawei Technologies, and Netscout to participate in this Forrester Wave, but they chose not to participate, and we could not make enough estimates about their capabilities to include them in the assessment as nonparticipating vendors.

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Solution evaluated
A10 Networks	Thunder TPS with aGalaxy TPS
Akamai Technologies	Akamai DDoS Mitigation
Alibaba Cloud	Alibaba Cloud
Amazon Web Services	AWS Shield
Cloudflare	Cloudflare DDoS Protection
Google	Cloud Armor
Imperva	DDoS Protection
Lumen	Lumen DDoS Mitigation Service; Lumen DDoS Hyper
Microsoft	Azure DDoS Protection
Neustar	UltraDDoS Protect
Radware	Radware DDoS Protection Service; Radware DefensePro

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **Cloudflare protects against DDoS from the edge, and fast.** Cloudflare prides itself on its global network. It often trumpets that it's the fastest, or one of the biggest, or one of the most interconnected. Its DDoS protection service benefits from enormous network capacity. Over time, the vendor has added more intelligence to categorize and mitigate malicious traffic. Cloudflare has historically offered a free tier of DDoS protection to consumers and the SMB market, but this report evaluates its enterprise offering. Cloudflare's mission is to help build a better internet and to make the impact of DDoS a thing of the past. Given the satisfaction cited by Cloudflare's customers, it is at least on track.

Customer references view Cloudflare's edge network as a compelling way to protect and deliver applications. Since the solution is entirely cloud-based and has no on-premises component, Cloudflare can provide fast onboarding. Reference customers say that Cloudflare's alerting options and alerting frequency can be improved, and those with heavy regulatory requirements may need to look closely to ensure that Cloudflare can meet their needs. Agile technology firms and those looking to extend network functionality to the edge should look at Cloudflare.

- **Radware knows DDoS attacks better than anyone.** Longtime DDoS protection vendor Radware is making the jump from on-premises protection to cloud-delivered and hybrid. The vendor can sell appliances for those that want them. It can deliver DDoS protection from its own network of 13 scrubbing centers with over 5 Tbps of scrubbing capacity, or organizations can buy the service that's integrated into AWS and Azure.

  As one of the two vendors in this Forrester Wave offering a hardware appliance, Radware brings forward its deep technical understanding and mitigation of DDoS attacks. The vendor has a detection and response capability that can detect zero-day attacks and create real-time, custom signatures to mitigate them within 18 seconds or less. One customer reference interviewed for this research said of Radware: "[They are] a great partner. I wanted a company that could be engaged with me in the trenches. They will drop everything to assist me." Reference customers using Radware DDoS protection value its adjacent layer 7 security services like WAF and bot management. However, customer references were less enthusiastic about Radware's pricing model. Enterprises needing a DDoS specialist for the most difficult cases should look at Radware.

- **Akamai Technologies delivers premium service, in both senses of the word premium.** Like other evolving CDN companies, Akamai sells three kinds of DDoS protection; one tied to web-based application security (Kona Defender); a cloud-based authoritative domain name system service (Edge DNS); and its original Prolexic, which is the service reviewed in this evaluation. Akamai has more scrubbing centers than its non-CSP competitors, and therefore, impressive capacity — more than 175 Tbps of total network capacity.

  Reference customers like the professionalism, engineering, and expertise of Akamai's Prolexic service. One reference said that Akamai's "assistance in a DDoS attack is outstanding. They are there to support your needs at any time and provide notice of other attacks that may be occurring [in] your business vertical." Akamai boasts an impressive analytics dashboard, for customers who need visibility (and there are some). However, those with shallower pockets complain that the solution is pricey. In answer to that, Akamai offers a "safe driver" discount for customers that had no attacks in the prior term. Large enterprise clients that want an experienced, trusted vendor to make their DDoS problem go away should look to Akamai.

- **Imperva delivers DDoS protection in an application security suite.** Imperva is an application security specialist vendor that fields a distributed global network to manage DDoS attacks combined with its own custom appliances (Behemoths) in its data centers to handle the heavy lifting of fighting DDoS attacks. Imperva's vision is "protecting data and all the paths to it," on which it delivers in terms of protection from DDoS attacks.

  Where Imperva's network capacity was a strength in past years, the capacity of its competitors has caught up and, in many cases, surpassed Imperva's (though all of them are sufficient to deter large volumetric attacks ... for now). Reference customers cite the company's improved support and say that the adjacent application security products (like WAF and bot management) are a factor in why they stay with Imperva, even when protecting public cloud-based applications. Midsize retail and financial services firms and those with additional application security requirements should evaluate Imperva for DDoS protection.

Strong Performers

- **AWS Shield Advanced is more than good enough for advanced AWS orgs.** AWS Shield Advanced protection caught our attention when it deflected a massive 2.3 Tbps attack in Q1 2020.[4] But putting scale aside for the moment, the compelling draw for AWS Shield Advanced protection is that it's already in front of customers' AWS-hosted applications, and there's no need to get another vendor approved and to maintain another vendor relationship. The vision for AWS is to keep applications available and responsive, and the associated DDoS roadmap is very technical and low-level. The convenient proximity of Shield Advanced is clearly drawing many customers, giving AWS a large market presence.

  However, the AWS solution requires that customers be very educated about the internals of AWS objects that are used to affect the protection. For example, customers need to know which S3 buckets their logs are going into so that they can provide access to those buckets to the Amazon response team when necessary. Alerting is handled by AWS Cloudwatch. AWS relies on its WAF to provide layer 7 protection, so it is bundled Shield Advanced. However, some customers can't (or won't) put WAFs in front of an object they want to protect, meaning that it has to go without layer 7 protection. While pricing for Shield Advanced is quite clear — a relatively small, fixed cost *per organization (no matter how many separate accounts)* — one customer reference cited excessive costs related to high-volume services. Enterprises already invested with AWS and that have solid expertise navigating its infrastructure will benefit from evaluating Shield Advanced for DDoS protection.

- **A10 Networks brings big iron to on-premises DDoS protection.** A10 Networks has new management and a new logo (with a dreamy mauve corporate color scheme). It's the only vendor in this Forrester Wave to rely on hardware sales for the vast majority of its DDoS-related revenue. The vendor can provide cloud-based volumetric DDoS protection through a partner if clients really need it, but A10 typically sells its customers (like ISPs and cloud providers) DDoS hardware appliances and management software. As a primarily on-premises infrastructure player, A10 caters to really large enterprises and service providers. Business is brisk at A10 as these fewer customers place large, large orders for A10's specialized solution.

A10 is deft at the technical aspects of threat detection and mitigation, with its AI/ML Zero-day Attack Protection (ZAP), adaptive baselining, and threat intelligence feeds. Customer references cite the performance and cost ratio of A10's DDoS protection appliances. A10's solution excels at protecting DNS and defending against the bursty attacks that are increasingly common today. The obvious mismatch for many enterprises is that A10 leads with an on-premises solution, but the majority of Forrester clients are looking to consume DDoS protection as a service. Large enterprises with heavy data center investments, gaming companies, CSPs, ISPs, and hosting providers should look to A10's Thunder TPS to build out DDoS scrubbing services for their customers.

Contenders

- **Google offers scale now and AI in the future.** Even at cloud scale, Google impresses. The vendor supports 24 regions (with another nine coming), nearly 150 worldwide points of presence, and an infrastructure that can absorb a 2.5 Tbps attack.[5] With this scale, Google can protect applications hosted within Google Cloud Platform (GCP) and also provide protection to external applications and services. Elements of the GCP DDoS roadmap are fundamental, as they're playing catch-up to the established competition. For example, GCP has machine learning for application layer DDoS on its roadmap for 2021, but the capability wasn't available during our evaluation.

  Reference customers cite the speed and professionalism of the Google engineers helping them with attacks, along with the ability to use Big Query for log analysis. However, they also say that network attack visibility is lacking. Enterprises already invested in the GCP ecosystem, for example those using Kubernetes at GCP, will find Google's Cloud Armor the ready option, as it's built into the GCP infrastructure where the application already lives.

- **Microsoft uses its vast threat intelligence to protect clients.** Microsoft uses insights from more than 200 global cloud and commercial services to collect a vast amount of DDoS threat intelligence. The logic is, if Microsoft can defend its global footprint, then it can defend clients as well. Many organizations are likely to consider Microsoft's DDoS solution because it's already part of the cloud infrastructure where they host applications or services. The general cloud service provider model has DDoS protection "always on," and Microsoft's is no exception. What is different is that Microsoft's is not inline, meaning that it can detect a DDoS attack happening but has to signal to its mitigation technology to initiate defense. The vendor's roadmap includes addressing this awkwardness and making mitigation always inline.

  Microsoft Azure's breadth of regulatory compliance coverage is also vast, and it has a unique compliance dashboard to help when auditors come calling. Customer references cite the ease of configuration, onboarding, and price transparency as strengths for Microsoft's DDoS service. Customer references also indicate that they'd prefer layer 7 protection that did not involve

Microsoft's WAF. Organizations that have invested workloads into Azure and have a need for infrequent DDoS protection against middling attackers should give Microsoft's DDoS protection a good look.

- **Alibaba Cloud enlists ML in service of DDoS protection.** Like the other cloud service providers, Alibaba Cloud offers a DDoS protection solution whose biggest attraction is that it's already part of its cloud infrastructure, making it a natural service for Alibaba Cloud's customers to consume. Also, Alibaba Cloud offers on-premises DDoS mitigation solutions. Two of Alibaba Cloud's scrubbing centers are in North America, two are in Europe, and seven more are in APAC. While Alibaba Cloud's service has over 10 terabits of scrubbing capacity today, 8 of that is in China, where most of its customers are located. Alibaba Cloud's roadmap is tactical — increasing capacity and broadening coverage. The vendor also has its eye on future technologies like 5G networks.

  Alibaba Cloud's core strength is AI/ML expertise, which it applies topically (after baselining) to differentiate malicious traffic from legitimate traffic. The vendor uses this technique across layer 3, layer 4, and layer 7 traffic. Last year, the AI automatically foiled a 5 million query per second (QPS) attack against a customer. While Alibaba Cloud is proud of its five different pricing models for DDoS protection, customer references report confusion with the selection and would prefer a simpler approach. Enterprise customers already invested in the Alibaba Cloud will find the vendor's DDoS service a natural fit to their applications.

- **Neustar specializes in protecting snowflakes.** Neustar is a veteran in the DDoS protection market, having first built DDoS protection for its UltraDNS services and then making it generally available. In 2018, Neustar acquired the DDoS and DNS services of another DDoS protection vendor, Verisign.[6] While other vendors have shiny visions, Neustar focuses on bespoke configurations, treating every customer like the unique snowflake that they are, each with their own way of doing border gateway protocol (BGP) announcements.

  One customer interviewed for this research said that Neustar was the fastest to get them a response during an attack (protection in 2 hours), and that they've been satisfied with Neustar since. While Neustar is good with mitigating the attacks, it's not great at reporting, dashboarding, and SIEM integration. This makes it difficult to show ongoing value when cost cutters come around. Neustar has an excellent service-level agreement and great service-delivery options that align to its true strength: handling bespoke environments. Organizations seeking a very flexible vendor that is easy to work with, has seen every kind of configuration, and is likely to go the extra mile on a budget should look at Neustar.

- **Lumen provides a cost-effective, hands-free, and easy button for customers.** The carrier previously known as CenturyLink is now Lumen, but the vendor still lays claim to having one of the, if not the, largest peered network on the planet. Lumen leverages its ownership of that giant network to not only protect services from network DDoS attacks but to also detect and shut down bots squatting therein. Lumen is the only vendor to have not one, not two, but an unheard-of three levels of scrubbing centers.

Customers interviewed for this research like how Lumen fully manages the solution and praised its customer service, both during onboarding and during attack. Clients calling during an incident receive a human response within 30 seconds, as testified by one customer reference who timed it. One drawback of Lumen's current offering is its reliance on application security controls like web application firewalls for layer 7 defense — for some applications those controls make sense, but not for all. Organizations using Lumen as an enterprise carrier as well as price-sensitive customers looking to protect network services should look at Lumen's DDoS protection.

Evaluation Overview

We evaluated vendors against 28 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include volumetric scrubbing, public cloud asset protection, detection and attack mitigation, security operations centers, response automation, speed of implementation, alerting, regulatory compliance, service delivery, on-premises component, service agreements, and threat intelligence.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, planned enhancements, performance, pricing model, and development and support.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's current revenue and installed base.

Vendor Inclusion Criteria

Forrester included 11 vendors in the assessment: A10 Networks, Akamai Technologies, Alibaba Cloud, Amazon Web Services, Cloudflare, Google, Imperva, Lumen, Microsoft, Neustar, and Radware. Each of these vendors has:

- **Significant market presence.** Vendors in this Forrester Wave generated $50 million or more in DDoS product and services sales in 2019.
- **Presence in more than one global region.** Vendors in this Forrester Wave have demonstrated that they generated 20% or more revenue outside their primary region.
- **Forrester mindshare.** Forrester considered level of client interest based on various interactions, including inquiries and advisories.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by November 20, 2020 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ and New Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] See the Forrester report "The Forrester Wave™: DDoS Mitigation Solutions, Q4 2017."

[2] Base: 1,059 global security decision-makers with network, data center, app security, or security ops responsibilities and who are responsible for customer/employee identity access management (at companies of 20-plus employees). Source: Forrester Analytics Business Technographics® Security Survey, 2020.

[3] Alibaba Cloud sold an anti-DDoS service as early as 2016. AWS did not make DDoS protection generally available until November 2017.

[4] Source: "AWS Shield Threat Landscape Report – Q1 2020," AWS Shield (https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf).

[5] Source: Damian Menscher, "Exponential growth in DDoS attack volumes," Google Cloud Blog, October 17, 2020 (https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks).

[6] Source: "Neustar to Acquire Verisign's Security Services Customer Contracts," Neustar, October 25, 2018 (https://www.home.neustar/about-us/news-room/press-releases/2018/VerisignSecurityServices).

FORRESTER®

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

› Core research and tools
› Data and analytics
› Peer collaboration
› Analyst engagement
› Consulting
› Events

Forrester’s research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
• Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.