The Forrester Wave™: DDoS Mitigation Solutions, Q4 2017

Tools And Technology: The Security Architecture And Operations Playbook

by Joseph Blankenship

December 7, 2017

Why Read This Report

In our 36-criteria evaluation of DDoS mitigation providers, we identified 11 of the most significant ones — Akamai Technologies, Arbor Networks, Cloudflare, F5 Networks, Fortinet, Huawei Technologies, Imperva, Neustar, Nexusguard, Radware, and Verisign — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Imperva, Cloudflare, Radware, Akamai, And Arbor Networks Lead The Pack

Forrester's research uncovered a market in which Imperva, Cloudflare, Radware, Akamai Technologies, and Arbor Networks lead the pack. Neustar, Verisign, Nexusguard, and F5 Networks offer competitive options. Huawei Technologies and Fortinet lag behind.

S&R Pros Are Looking For Strong Detection And Mitigation Capabilities

The distributed denial of service (DDoS) mitigation solution market is growing because more S&R professionals understand that DDoS attacks are a threat to their digital businesses. Forrester's research has found that having a DDoS mitigation solution in place is a best practice to protect internet-facing websites, applications, and infrastructure.

Scrubbing Capacity, On-Premises Solutions, And SSL Investigation Are Differentiators

DDoS attacks originate all over the world. Cloud-based services need scrubbing capacity close to the origin in order to stop attacks before they affect the network. Hybrid deployments require the capability to work with on-premises equipment. As more internet traffic is SSL encrypted, it's imperative that DDoS mitigation solutions are able to examine SSL traffic to detect attacks.

The Forrester Wave™: DDoS Mitigation Solutions, Q4 2017

Tools And Technology: The Security Architecture And Operations Playbook

by Joseph Blankenship
with Stephanie Balaouras, Bill Barringham, and Shayna Neuburg

December 7, 2017

Table Of Contents

Related Research Documents

Predictions 2018: Cybersecurity

Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet

TechRadar™: Zero Trust Network Threat Mitigation Technologies, Q4 2016

FORRESTER®

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

DDoS Mitigation Is Essential To Protect Your Digital Business

Digital businesses depend on constant, uninterrupted connectivity. Websites, applications, and cloud services are potential targets for DDoS attacks. Attackers may target enterprises for extortion, hacktivism, political motivation, competitive reasons, or as part of a data breach.[1] According to a recent survey, 24% of global enterprises that suffered a data breach over the past 12 months were victims of a DDoS attack.[2] No matter the motivation, DDoS attacks can significantly harm or even cripple digital businesses. S&R pros should consider that:

- **Customers demand instant access to content.** Customers don't have patience for site outages or slow performance. According to Forrester data, 58% of global security decision makers at enterprise firms reported that they are highly concerned about an IT outage affecting customer-facing systems.[3] An outage or slow-performing site can negatively affect customer experience and the bottom line. For example, internet giant Google found that 53% of mobile users abandon sites that take more than 3 seconds to load.[4]
- **Cloud service adoption requires constant availability.** In an interconnected world, systems and applications require continuous connectivity to cloud services. Disruptions or latency upstream can have dire consequences on sensitive applications downstream. The 2016 Mirai botnet attack against domain name system (DNS) provider Dyn demonstrated the devastating downstream potential that DDoS attacks can have on businesses that rely on Dyn for DNS services.[5]

On-Premises, Cloud, And Hybrid DDoS Models Provide Protection Options

Enterprises have various options for DDoS mitigation. Firewalls and intrusion prevention systems come with some DDoS mitigation capability built in, but these solutions can be overwhelmed by large attacks or circumvented by clever attackers. Internet service providers (ISPs) and managed security services providers (MSSPs) may offer DDoS mitigation as part of their services, but those without dedicated DDoS services and personnel may not have the needed expertise when there is a massive, complex attack against the enterprise. S&R pros evaluating DDoS mitigation solutions should know:

- **On-premises solutions deliver downstream protection.** Companies with extensive on-premises infrastructure that are in high-risk industries like financial services or retail may choose DDoS product solutions deployed as appliances. DDoS protection appliances can quickly defend against most DDoS attacks without creating latency.
- **Cloud DDoS mitigation services provide upstream protection.** Firms with very distributed infrastructure, cloud-hosted assets, or a cloud-first strategy may choose cloud-based DDoS mitigation. Content delivery network (CDN) providers and DNS providers have massive network bandwidth and high-capacity DDoS scrubbing capabilities. These services stop DDoS attacks before they reach your network or cloud-hosted assets. You can choose on-demand or always-

on mitigation (at a much higher cost) to get the right level of protection for your needs. Seventy-four percent of global survey respondents indicated that their enterprise firms have either already implemented DDoS-as-a-service or are expanding/upgrading their implementation.[6]

› **Hybrid solutions offer the best of both.** Many firms choose a hybrid approach using on-premises DDoS mitigation appliances with cloud-based services. A hybrid approach provides fast detection and defense with low latency with the ability to utilize cloud-based mitigation should the need arise. When attack volumes grow and threaten to overwhelm the on-premises solution, it can signal to the cloud provider to begin mitigation in the cloud.[7]

DDoS Mitigation Solutions Evaluation Overview

To assess the state of the DDoS mitigation solution market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of the top vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 36 criteria, which we grouped into three high-level buckets:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave™ graphic indicates the strength of its current offering. Our evaluation of the current offering focused on its ability to detect and mitigate multiple attack types, mitigation capacity, service levels, threat intelligence, reporting, visibility, and client satisfaction. We also evaluated the extent to which vendors based their solution on their own intellectual property (IP) and the technology partners they used to deliver aspects of the solution.

› **Strategy.** A vendor's position on the horizontal axis of the Forrester Wave graphic indicates our assessment of its strategy. We evaluated vendors' road map, partner ecosystem, global presence, pricing, and staffing.

› **Market presence.** The size of each vendor's bubble on the Forrester Wave graphic indicates the vendor's market presence. We evaluated vendors' current revenue, revenue growth, and DDoS installed base.

Evaluated Vendors And Inclusion Criteria

Forrester included 11 vendors in the assessment: Akamai Technologies, Arbor Networks, Cloudflare, F5 Networks, Fortinet, Huawei Technologies, Imperva, Neustar, Nexusguard, Radware, and Verisign. Each of these vendors has (see Figure 1):

› **A complete DDoS mitigation solution.** We included providers that offer a complete DDoS mitigation solution made up of products, services, or a combination of products and services that blocks attempts to render computer resources (e.g., websites, email services, VoIP, or whole networks) unavailable to users.

- **Presence in more than one global region.** To be included, the provider had to have a strong or growing presence for DDoS mitigation in North America as well as at least one other global region (Latin America, Europe, or Asia Pacific). Many large companies are participants in this Forrester Wave, but we focused only on their DDoS solution business.
- **A significant portion of the solution based on the vendor's own IP.** Forrester only included providers that have invested in their own IP and don't rely on third-party technology for the majority of the solution. As a result, we don't include many of the MSSPs and telcos that have DDoS services as part of their portfolios.
- **Significant interest from Forrester customers.** Forrester considered the level of interest from our clients based on our various interactions, including inquiries, advisories, and consulting engagements. Forrester has seen market interest for all vendors in this Forrester Wave.
- **A large installed base of enterprise DDoS customers.** The vendor needed to demonstrate a large installed base of enterprise DDoS customers with a significant part of its business revenue coming from DDoS protection services.

FIGURE 1 Evaluated Vendors: Product Information And Selection Criteria

Vendor	DDoS mitigation delivery	Product name
Akamai Technologies	As-a-service	Kona Site Defender, Web Application Protector, Prolexic Routed/Proxy, Fast DNS
Arbor Networks	Hybrid	Arbor APS, Arbor Cloud
Cloudflare	As-a-service	Cloudflare
F5 Networks	Hybrid	DDoS Hybrid Defender 13.2.0, Silverline DDoS Protection, DDoS Protection for BIG-IP
Fortinet	On-premises appliance	FortiDDoS
Huawei Technologies	Hybrid	Cloud Mitigation Service, AntiDDoS8000 series, and AntiDDoS1600 series appliances
Imperva	As-a-service	Incapsula
Neustar	Hybrid	SiteProtect 5.3.2
Nexusguard	Hybrid	Application Protection, Origin Protection, and DNS Protection 3.0
Radware	Hybrid	DefensePro 8.14, DefenseFlow 2.8, Cloud DDoS Protection Service 9.0
Verisign	As-a-service	DDoS Protection Services

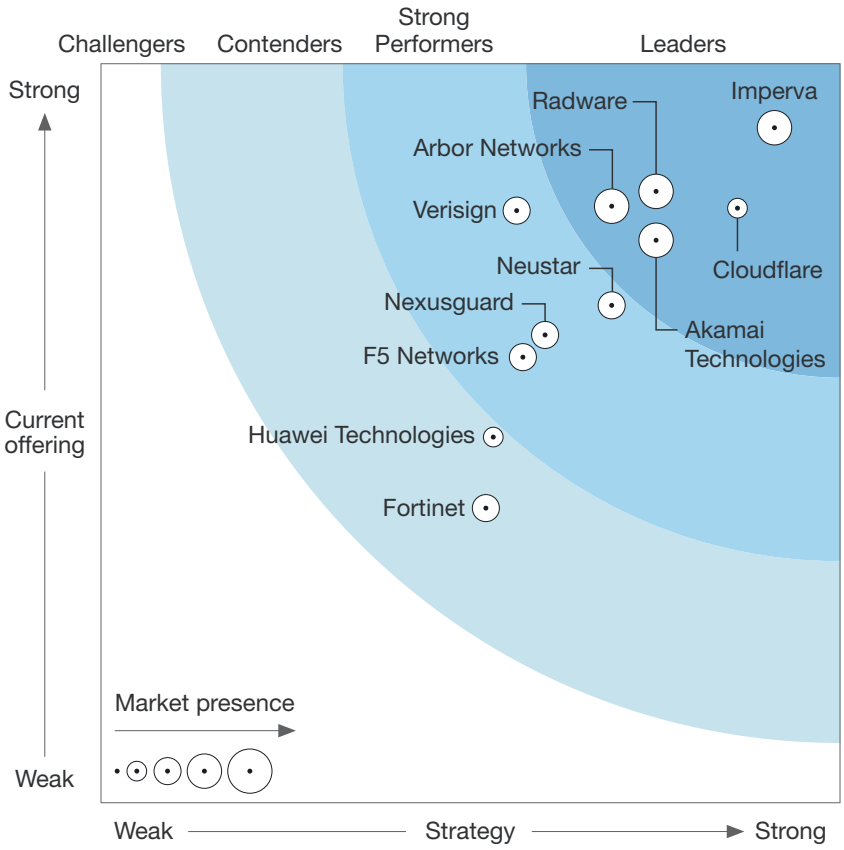
Vendor inclusion criteria

1. A complete DDoS mitigation solution.
2. Presence in more than one global region.
3. A significant portion of the solution based on the provider's own intellectual property (IP).
4. Significant interest from Forrester customers.
5. A large installed base of enterprise DDoS customers.

Vendor Profiles

This evaluation of the DDoS mitigation solution market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 2).

FIGURE 2 Forrester Wave™: DDoS Mitigation Solutions, Q4 2017



FORRESTER® **RESEARCH**
The Forrester Wave™

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

FIGURE 2 Forrester Wave™: DDoS Mitigation Solutions, Q4 2017 (Cont.)

	Forrester's weighting	Akamai Technologies	Arbor Networks	Cloudflare	F5 Networks	Fortinet	Huawei Technologies	Imperva	Neustar	Nexusguard	Radware	Verisign
Current Offering	50%	3.84	4.03	4.02	3.01	1.99	2.47	4.56	3.36	3.16	4.13	4.00
Scrubbing centers	4%	5.00	2.00	5.00	1.00	1.00	4.00	5.00	3.00	3.00	3.00	2.00
Security operations centers (SOCs)	4%	5.00	2.00	4.00	2.00	1.00	3.00	5.00	2.00	3.00	3.00	2.00
Length of implementation	3%	4.00	4.00	5.00	3.00	0.00	1.00	5.00	3.00	3.00	3.00	4.00
Professional services	3%	5.00	5.00	4.00	4.00	2.00	1.00	5.00	2.00	3.00	4.00	4.00
Layers 3 and 4 attack mitigation	4%	4.00	5.00	5.00	3.00	3.00	2.00	5.00	3.00	3.00	4.00	5.00
Layer 7 attack mitigation	4%	5.00	4.00	3.00	4.00	2.00	2.00	5.00	3.00	3.00	5.00	4.00
DNS attack mitigation	4%	3.00	4.00	5.00	4.00	2.00	3.00	5.00	4.00	3.00	5.00	5.00
Internet-of-things (IoT) botnets	4%	3.00	4.00	5.00	3.00	2.00	2.00	5.00	3.00	3.00	5.00	5.00
Detection tactics	4%	3.00	4.00	4.00	3.00	3.00	3.00	4.00	3.00	3.00	5.00	4.00
Multivector attacks	4%	4.00	3.00	5.00	4.00	3.00	2.00	5.00	5.00	3.00	5.00	5.00
New attack types	4%	4.00	3.00	4.00	3.00	2.00	1.00	5.00	4.00	2.00	4.00	4.00
Latency	4%	5.00	5.00	4.00	3.00	2.00	1.00	5.00	3.00	3.00	4.00	4.00
Service delivery	4%	5.00	5.00	4.00	3.00	2.00	2.00	5.00	3.00	5.00	4.00	5.00
On-premises solution	4%	1.00	5.00	1.00	3.00	4.00	4.00	0.00	4.00	2.00	5.00	2.00
Service levels	4%	4.00	5.00	4.00	2.00	2.00	2.00	5.00	3.00	3.00	3.00	5.00
Filtering deployment	4%	4.00	4.00	5.00	3.00	3.00	3.00	4.00	4.00	3.00	4.00	4.00
Response automation	4%	3.00	4.00	4.00	3.00	1.00	2.00	5.00	4.00	3.00	4.00	4.00
Secure socket layer (SSL) investigation	3%	4.00	4.00	5.00	5.00	0.00	2.00	4.00	5.00	2.00	5.00	5.00
Mitigation capacity	4%	5.00	3.00	5.00	3.00	2.00	2.00	4.00	4.00	3.00	3.00	3.00
Intellectual property (IP)	3%	4.00	5.00	5.00	4.00	5.00	5.00	5.00	3.00	4.00	5.00	4.00
Technology partners	3%	4.00	4.00	5.00	2.00	3.00	4.00	5.00	3.00	4.00	4.00	5.00
Threat intelligence	5%	5.00	5.00	4.00	3.00	2.00	4.00	4.00	4.00	4.00	3.00	3.00
Portal	5%	3.00	5.00	4.00	3.00	1.00	2.00	5.00	3.00	4.00	4.00	4.00

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

FIGURE 2 Forrester Wave™: DDoS Mitigation Solutions, Q4 2017 (Cont.)

	Forrester's weighting	Akamai Technologies	Arbor Networks	Cloudflare	F5 Networks	Fortinet	Huawei Technologies	Imperva	Neustar	Nexusguard	Radware	Verisign
Current Offering	50%	3.84	4.03	4.02	3.01	1.99	2.47	4.56	3.36	3.16	4.13	4.00
Telemetry	3%	3.00	5.00	2.00	3.00	2.00	2.00	5.00	3.00	4.00	5.00	5.00
Reporting	4%	3.00	3.00	2.00	2.00	1.00	3.00	4.00	3.00	3.00	5.00	4.00
Visibility	4%	2.00	3.00	2.00	3.00	1.00	2.00	5.00	3.00	3.00	4.00	4.00
Strategy	30%	3.75	3.45	4.30	2.85	2.60	2.65	4.55	3.45	3.00	3.75	2.80
Planned enhancements	30%	5.00	3.00	5.00	3.00	2.00	3.00	5.00	4.00	5.00	3.00	4.00
Geographical markets	15%	4.00	4.00	5.00	4.00	2.00	3.00	5.00	3.00	2.00	4.00	3.00
Pricing model	20%	1.00	4.00	5.00	3.00	3.00	3.00	4.00	3.00	3.00	3.00	4.00
Development and technical staffing	15%	5.00	3.00	3.00	1.00	2.00	2.00	4.00	5.00	2.00	5.00	1.00
Account management staffing	10%	5.00	3.00	3.00	1.00	4.00	4.00	4.00	2.00	1.00	4.00	1.00
Value-added resellers (VARs)	5%	4.00	5.00	1.00	5.00	5.00	0.00	5.00	4.00	2.00	5.00	1.00
Service and system integrators (SIs)	5%	0.00	3.00	5.00	5.00	3.00	0.00	5.00	1.00	2.00	5.00	1.00
Market Presence	0%	3.67	4.00	1.67	2.33	3.00	2.00	3.67	2.67	2.67	4.00	2.67
Current revenue	33%	5.00	5.00	1.00	4.00	5.00	2.00	4.00	3.00	2.00	5.00	3.00
Revenue growth	33%	3.00	5.00	1.00	1.00	2.00	2.00	3.00	2.00	4.00	2.00	2.00
Installed base	33%	3.00	2.00	3.00	2.00	2.00	2.00	4.00	3.00	2.00	5.00	3.00

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

Leaders

› **Imperva.** Imperva offers DDoS mitigation services as part of its cloud security and CDN portfolio. The company was among the top ranked in this study for its ability to detect and mitigate layer 3, 4, and 7 attacks, DNS attacks, internet-of-things (IoT) botnet attacks, and new attack types, as well as for its scale and speed. It also received some of the highest customer ratings in this study for overall satisfaction with the solution, value, overall usability, and vendor relationship. Imperva has a large customer install base and significant global presence, with scrubbing centers in all four geographies.

The company doesn't offer an on-premises solution and doesn't plan to offer one in the future. Future plans include speeding the onboarding process, developing customer-defined analytics, and expanding network mitigation capacity. The only area where customers rated Imperva below the peer group average was for overall solution cost. Large, global enterprises needing a reliable, scalable, and highly effective cloud-based DDoS solution should consider Imperva.

- **Cloudflare.** Cloudflare provides a CDN, web application firewall (WAF), and DDoS mitigation services. Cloudflare has a large global footprint, with coverage in all four geographies. The solution relies on its vast scale and a high degree of automation to stop attacks. Customers rated it highly for its ability to mitigate layer 3 and 4 attacks as well as DNS attacks and new attack types. Weaknesses noted by customers include reporting, ability to control mitigation efforts, and authentication. The company's road map includes enhanced layer 7 detection, expanded protocol protection, traffic analytics, and the use of artificial intelligence for detection. Enterprises that need a more automated, hands-off approach to DDoS mitigation or want to combine multiple services should consider Cloudflare.
- **Radware.** Radware is a cybersecurity vendor that delivers on-premises and cloud-based DDoS mitigation solutions. Many service providers and telcos use Radware technology as the basis of their DDoS mitigation services. On-premises appliances can be combined with Radware's cloud DDoS mitigation service for a hybrid solution. The company is among the top performers for layer 7 and DNS defense as well as the ability to fend off multivector attacks. Radware has a strong global presence, with multiple security operations centers (SOCs) and scrubbing centers in three geographies. Customer references remarked on the solution's reliability, behavioral detection capabilities, and ability to scale. Customers commented about the strength of US support but noted that overseas support is not as strong. The company also rated below the peer group average for pricing, the ability to create custom dashboards, and interactions with SOC personnel. Road map items include expanded protection against IoT botnet, DNS, and burst attacks. Large, global enterprises and service providers with a need for on-premises solutions or a hybrid approach for DDoS mitigation should consider Radware.
- **Akamai Technologies.** Akamai, one of the largest global CDNs, offers DDoS mitigation services alongside its delivery, performance, and cloud security solutions. The company delivers DDoS mitigation services via its CDN-based Kona Site Defender solution and its Prolexic DDoS scrubbing service. These services integrate with the company's WAF and DNS services. Akamai received favorable feedback on its ability to detect new attack types while yielding few false positives. Reference customers remarked on the company's responsiveness, expertise, and ability to immediately stop attacks. Akamai rated the lowest out of the peer group for pricing and overall solution cost, with customer references stating that cost, affordability, and visibility into the pricing structure are challenges. Future plans call for expanded mitigation capacity, enhanced detection capabilities, increased visibility, and improved workflow. Large enterprises that need global CDN capabilities with proven DDoS mitigation expertise should consider Akamai Technologies.

› **Arbor Networks.** Arbor Networks is a focused DDoS protection provider. Many service providers and telcos rely on Arbor Networks technology to power their DDoS mitigation services. Arbor is best known for its premises-based DDoS mitigation appliances, but it has grown its cloud-based DDoS mitigation services through a partnership with Neustar that can work alone or in conjunction with premises-based appliances for a hybrid approach. The vendor rated higher than the peer group average for its ability to defend against layer 3, 4, and 7 attacks. Clients gave Arbor high marks for value delivered, overall solution cost, and vendor-provided threat intelligence. Arbor currently has only one SOC, located in North America, and a limited number of global scrubbing centers. The mitigation capacity for the cloud offering is less than options from the cloud and CDN-focused vendors evaluated, although the road map calls for additional capacity to be added. Large enterprises and service providers that require an on-premises or hybrid approach for DDoS mitigation should consider Arbor Networks.

Strong Performers

› **Neustar.** Neustar is a provider of cloud-based information, data analytics, and security services. Its security services include DNS protection, IP reputation intelligence, and DDoS mitigation. The company delivers DDoS mitigation via its cloud-based SiteProtect service and partners with Arbor Networks to deliver a hybrid solution. The company operates one global SOC but has scrubbing centers in three of the four geographies. Currently, Neustar relies heavily on technology partners to deliver DDoS mitigation, although future plans call for the company to develop its own proprietary technology, expand network mitigation capacity significantly, and broaden its global reach. We were unable to adequately assess Neustar's current offerings due to limited client references. Enterprises seeking cloud-based DDoS services should consider Neustar.

› **Verisign.** Verisign is a leading operator of internet infrastructure. The firm's network infrastructure and security portfolio includes DNS solutions in addition to DDoS mitigation services. The company uses its own, internally developed Athena Shield technology to mitigate DDoS attacks. Hybrid capability is delivered via its OpenHybrid API that integrates with existing on-premises and cloud-based technologies. Client references report that Verisign delivers effective monitoring with low false positives and low latency. Customers rated Verisign higher than the peer group average for level 3, 4, and 7 attack mitigation as well as DNS attack mitigation. Weaknesses reported by clients include custom reporting and vendor-provided threat intelligence. Verisign has fewer scrubbing centers than the peer group average, but it has scrubbing centers in three geographies along with two SOCs to support its services. Road map items include expanding its global presence, increasing network mitigation capacity, and addressing the needs of underserved global markets with a turnkey scrubbing center solution. Enterprises with requirements for a reliable, cloud-based DDoS mitigation service provider that integrates with their existing infrastructure should consider Verisign.

› **Nexusguard.** Nexusguard is a DDoS pure play, offering DDoS mitigation along with application and DNS protection services. Customer references gave the firm solid marks for detecting and mitigating level 3, 4, and 7 attacks and for latency. Customers also rated Nexusguard well

for overall satisfaction with the solution, account management, workflow, automation, control over mitigation, and speed to mitigation. The firm partners with Huawei Technologies for hybrid deployments. Customer references scored the firm below the peer group average for detection and mitigation of IoT botnet attacks and new attack types — both are the focus of planned enhancements. The geographic presence of technical staff, sales, and partners is limited to one region: Asia Pacific. The firm's future plans call for architectural enhancements to speed protection, analytics to improve detection, and expanded threat intelligence capabilities. Enterprises based in Asia Pacific — with or without a global presence — that require reliable DDoS service from a focused provider should consider Nexusguard.

› **F5 Networks.** F5 is well known for its application delivery networking and application security solutions. It offers DDoS mitigation through its on-premises Herculon DDoS Hybrid Defender solution or its cloud-based Silverline DDoS mitigation service — or it can combine the offerings for a hybrid solution. The company's DDoS mitigation offerings are sold standalone or in conjunction with its WAF and application delivery solutions. F5 has the fewest scrubbing centers and the lowest network mitigation capacity out of the companies evaluated in this study. We were unable to adequately assess F5's current offerings due to limited client references. The company's future plans call for increased analytics, intelligence sharing, and improved reporting. Enterprise clients seeking a hybrid solution to protect on-premises and cloud-based assets should consider F5 Networks.

Contenders

› **Huawei Technologies.** Huawei is a networking solution provider that delivers DDoS mitigation through on-premises appliances. Many of its clients are service providers and large enterprises that require highly scalable solutions for DDoS mitigation. Customer references noted the solution's capacity and ability to defend against attacks automatically. In most categories, however, customer references rated the company below the peer group average. Shortcomings mentioned by customers include the need to configure some policies through a command line interface, ability to defend against layer 7 attacks, and delays in attack detection. Huawei partners with Nexusguard and China Telecom to provide a hybrid DDoS mitigation solution. The company has a strong customer base in Asia Pacific and Europe, but it has little presence in North America. Huawei sells directly, instead of working with value-added resellers or system integrators to sell and integrate its solutions. The company's road map includes expanded mitigation capacity, enhanced protection from multivector attacks, and increased scaling in the cloud. Large enterprises and service providers with a strong presence in Asia Pacific and Europe that need on-premises DDoS mitigation should consider Huawei.

› **Fortinet.** Fortinet is best known as one of the leading network security providers. The firm offers a dedicated, inline, on-premises DDoS appliance, FortiDDoS, built with its own IP. Fortinet partners with Verisign for a cloud-based DDoS offering for those customers requiring a hybrid solution. The company has deliberately chosen not to develop its own cloud-based solution in order to avoid competing directly with its own customers, many of whom are MSSPs, ISPs, and others

that offer their own cloud solutions. Customer references gave Fortinet positive feedback for detecting and mitigating layer 3 and layer 4 attacks, as well as for its on-premises implementation services and ongoing technical support. One shortcoming of the standalone Fortinet DDoS solution is that it cannot inspect SSL traffic. Customers rated the firm below-average for reporting and visibility in areas ranging from the ability to customize dashboards and reports to executive-level and compliance reporting. The company's future plans call for additional capacity with higher-bandwidth appliances and clustering, enhancements for MSSP partners, and centralized management. Existing enterprise and service provider clients of Fortinet that need an on-premises DDoS solution as part of their hybrid strategy should consider Fortinet.

Supplemental Material

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at Forrester.com at the beginning of this report to download.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by November 17, 2017.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference information.** To validate product and vendor qualifications, Forrester also surveyed three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and

market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

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

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2017 was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Data's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] The lines between activists, state actors, and cybercriminals are blurry. See the Forrester report "Know Your Adversary" and see the Forrester report "Achieve Early Success In Threat Intelligence With The Right Collection Strategy."

[2] This data was taken from survey responses of 245 global network security decision makers whose firms (employing 1,000 people or more) have had an external security breach in the past 12 months. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[3] This data was taken from survey responses of 1,700 global security decision makers employed at enterprise firms of 1,000 people or more. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[4] Source: Alex Shellhammer, "The need for mobile speed: How mobile latency impacts publisher revenue," DoubleClick, September 2016 (https://www.doubleclickbygoogle.com/articles/mobile-speed-matters/).

[5] See the Forrester report "Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet" and see the Forrester report "Top Cybersecurity Threats In 2017."

Source: Dave Lewis, "The DDoS Attack Against Dyn One Year Later," Forbes, October 23, 2017 (https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#427c4091ae9c).

[6] This data was taken from survey responses of 604 global network security decision makers working at enterprise firms of 1,000-plus employees. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[7] See the Forrester report "Develop A Two-Phased DDoS Mitigation Strategy."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

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.

137209