The Forrester Wave™: DDoS Services Providers, Q3 2015

Nine Vendors That Can Help You Protect Your Presence On The Web

by Rick Holland and Ed Ferrara

July 22, 2015 | Updated: UpdateJuly 23, 2015

Why Read This Report

In Forrester's 36-criteria evaluation of distributed denial of service (DDoS) services providers, we identified nine of the most significant companies — Akamai Technologies CenturyLink, CloudFlare, DOSarrest Internet Security, F5 Networks, Imperva, Level 3 Communications, Neustar, and Verisign — in a crowded field of competitors. We researched, analyzed, and scored them to determine which are best able to protect their customers' business. The DDoS services space is growing in importance because distributed denial of service attacks now represent a considerable percentage of the total number of threats against organizations of all sizes. DDoS has historically focused on disruption, but today it is more frequently an opening salvo for more complex attacks that result in theft of sensitive data or valuable intellectual property. This report details how well each vendor measures up against our criteria and against each other with their DDoS prevention services.

Key Takeaways

Akamai Technologies, CloudFlare, Imperva, CenturyLink, And Verisign Lead The Pack

Forrester's research uncovered a market in which Akamai Technologies, CloudFlare, Imperva, CenturyLink, and Verisign came out ahead as Leaders. F5 Networks Neustar, DOSarrest Internet Security, and Level 3 Communications offer competitive options and are Strong Performers.

The DDoS Services Market Can Provide All The DDoS Protection You Need

Outsourcing DDoS protection services is now ready for prime time. There is no need to consider implementing your own DDoS solution on-premises when there are a significant number of effective outsourcing partners that can offer better DDoS protection compared with what security and risk pros can do for themselves.

Complexity Reduction And Geographic Support Differentiate The Market

On-demand solutions requiring BGP or DNS routing changes add to the complexity of a DDoS protection service. One way to reduce complexity is to use an always-on model. Always-on doesn't need to add latency when coupled with good geographic support. The best firms offer both approaches with strong geographic presence to provide a complete solution.

The Forrester Wave™: DDoS Services Providers, Q3 2015

Nine Vendors That Can Help You Protect Your Presence On The Web

by Rick Holland and Ed Ferrara
with Christopher McClean, Christopher Mines, Claire O'Malley, and Peggy Dostie

July 22, 2015 | Updated: UpdateJuly 23, 2015

Table Of Contents

Notes & Resources

Forrester conducted service evaluations in March 2015 and interviewed nine vendor and user companies: Akamai Technologies, CenturyLink, CloudFlare, DOSarrest Internet Security, F5 Networks, Imperva, Level 3 Communications, Neustar, and Verisign.

Related Research Documents

The Forrester Wave™: SaaS Web Content Security, Q2 2015

The State Of The Cyberthreat Intelligence Market

TechRadar™: Application Security, Q2 2015

FORRESTER®

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

Customer-Facing Application Performance Influences DDoS Buyers

The DDoS services market has shown significant growth over the past two years. Much of this has been driven by the marked rise in DDoS attacks and the realization that these attacks are easy to launch and are often used as a diversion for the theft of intellectual property.[1] Just as importantly, in the Internet-driven and -connected economy, your web presence significantly influences how your customers view your organization and the products or services it provides. Security professionals considering how to justify DDoS prevention should ask, "What is our connection to the Internet worth?"

Multiple DDoS Service Models Provide Options

There are two primary modes of delivering DDoS services: on-demand and always-on. For both modes, vendors offer a hybrid option, so customers can use their own scrubbing facility for attacks that fall below a certain threshold of velocity and volume but can then fail over to the vendor during larger attacks. All of the vendors we reviewed provide all models of deployment; their preferred approach depends on their infrastructure, their provisioning process, the geographic location of the customer's data center and their scrubbing center, and their available bandwidth. Security professionals should consider the pros and cons of each option:

- **On-demand solutions provide defensive services only when needed.** On-demand solutions are manually or automatically started when either the customer or the vendor detects a DDoS attack. Vendors sell this mode when attack volume is low and the primary concern is application latency. The customer (or vendor acting on the customer's behalf) uses either BGP route changes or DNS redirection to send their network traffic through the vendor's infrastructure.
- **Always-on solutions don't require routing or DNS changes.** Always-on service models have the advantage of not needing to change BGP routing or DNS records. These solutions are best when there is a high frequency of attacks. Many of the providers that offer always-on solutions indicate they have little impact on application latency. They also have an advantage in that they work well with content delivery applications, as the vendor can bundle DDoS services with content delivery services.
- **Hybrid solutions offer the best of both worlds.** Hybrid solutions allow security pros to use their own on-premises DDoS scrubbing and web application firewalls as a first line of defense. When these facilities become overwhelmed, the customer can redirect traffic to the vendor's scrubbing center for additional remediation capacity.

DDoS Firms Deliver A Common Set Of Capabilities, With Differentiating Features

DDoS service providers help organizations of all sizes to protect against threats to online resources without having to incur extensive capital expenses or expanded headcount. All vendors in this market share core similarities; however, the best ones have clearly advanced features. They:

- **Offer application and network protection as their centerpiece.** DDoS attacks take on different forms; they may attempt to overwhelm web and application servers with a large amount of bogus network traffic, or they may launch attacks that attempt to confuse web applications with malformed server requests. The best DDoS service vendors can automatically detect both types of attacks and either provide an alert or automatically switch on to protect vulnerable websites (see Figure 1).
- **Support a broad set of protocols.** TCP-IP is the set of network communication protocols that allow the Internet to function, which means it can also bring applications and infrastructure to their knees when used as a weapon. The best DDoS service providers support a broad portfolio of device and protocol protection. More-narrowly focused providers only focus on a small set of protocols and devices. This could be problematic as hackers become more creative in their attack methods.
- **Defend networks and applications.** DDoS attacks are not just about the network anymore. Even though the frequency of application Layer 7 attacks is significantly less than that of their amplification Layer 3 and 4 attack cousins, these attacks do present big challenges to security pros now and will continue to do so in the future.
- **Employ talented sales, professional services, and technical staff.** One of the primary reasons for turning to a service provider for security staff is the quality of the people they bring to solving critical challenges. All of the vendors in this Wave have competent staff to address DDoS challenges (see Figure 2).
- **Maintain good networks of technology partners, resellers, and system integrators.** Security is a team sport, and because of the need for various types of skills, DDoS vendors also have a good network of technology and service partners to benefit their customers (see Figure 3).

FIGURE 1 Attack Types Defended, Response Tactics, And Protected Protocols

Vendor	Attack types defended	Response tactics	Protected network protocols
Akamai	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack via fast DNS, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate, highly volumetric AppSec, poison dart, slow POST, and origin error attacks	Attack source path identification, filtering, bandwidth throttling, reconfiguration, overprovisioning, router queue management, IP blacklisting, DNS recursion attenuation, malformed packet dropping	AMT, ARP, BGP, BOOTP, DHCP, DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, MVRP, NNTP, NTP, OSPF, PIM, POP, PPOe, PPP, PTP , RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL, others
CenturyLink	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate	Attack source path identification, filtering, bandwidth throttling, reconfiguration, overprovisioning, router queue management, IP blacklisting, DNS recursion attenuation, malformed packet dropping	AMT, ARP, BGP, BOOTP, DHCP, DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, MVRP, NNTP, NTP, OSPF, PIM, POP, PPOe, PPP, PTP, RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL, others
CloudFlare	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, non-isotropic attack traffic distribution, ping of death, reflector TCP reset, TCP SYN flooding, teardrop attack UDP flooding, varied rate	Attack source path identification, filtering, bandwidth throttling, reconfiguration, overprovisioning, router queue management, IP blacklisting, DNS recursion attenuation, malformed packet dropping	DNS, HTTP, HTTPS, SSH, SSL, TCP, others (WebSockets)
DOSarrest Internet Security	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate	Attack source path identification, filtering, bandwidth throttling, reconfiguration, overprovisioning, IP blacklisting, DNS recursion attenuation, malformed packet dropping	HTTP, HTTPS

FIGURE 1 Attack Types Defended, Response Tactics, And Protected Protocols (Cont.)

Vendor	Attack types defended	Response tactics	Protected network protocols
F5 Networks	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate, other: NTP, Sloworis, business layer attacks	Attack source path identification filtering, bandwidth throttling reconfiguration, overprovisioning, IP blacklisting, malformed packet dropping	BGP, DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, NTP, POP, RADIUS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS
Imperva	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate, headless browser attacks, CAPTCHA-solving botnets, XML bombs, NTP/DNS amplification	Attack source path identification, filtering, overprovisioning, IP blacklisting, DNS recursion attenuation, malformed packet dropping	AMT, ARP, BGP, BOOTP, DHCP, DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, MVRP, NNTP, NTP, OSPF, PIM, POP, PPOe, PPP, PTP, RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL
Level 3 Communi-cations	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, varied rate	Attack source path identification filtering, bandwidth throttling reconfiguration, overprovisioning, router queue management, IP blacklisting, malformed packet dropping	DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, NNTP, NTP, POP, RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL

FIGURE 1 Attack Types Defended, Response Tactics, And Protected Protocols (Cont.)

Vendor	Attack types defended	Response tactics	Protected network protocols
Neustar	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate, using regex filters-based on need	Attack source path identification, filtering bandwidth throttling, reconfiguration overprovisioning, router queue management IP blacklisting, DNS recursion attenuation, malformed packet dropping	AMT, ARP, BGP, BOOTP, DHCP, DNS, FTP, GRE, HTTP, HTTPS , ICMP, IMAP, MVRP, NNTP, NTP, OSPF, PIM, POP, PPOe, PPP, PTP, RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL, others (custom protocols, assuming the client provides packet sample information to Neustar in advance. IPV6 is not seen as a significant attack vector currently; however, the Neustar network is IPV6 compatible.)
Verisign	CGI request, denial of capability, diluted low rate degrading, direct, DNS request attack, high-rate disruptive, hybrid attack, ICMP attack, isotropic attack traffic distribution, land attack, mail bomb, non-isotropic attack traffic distribution, ping of death, reflector, TCP reset, TCP SYN flooding, teardrop attack, UDP flooding, varied rate	Attack source path identification, filtering, bandwidth throttling, reconfiguration, overprovisioning, router queue management, IP blacklisting, DNS recursion attenuation, malformed packet dropping	AMT, ARP, BGP, BOOTP, DHCP, DNS, FTP, GRE, HTTP, HTTPS, ICMP, IMAP, MVRP, NNTP, NTP, OSPF, PIM, POP, PPOe, PPP, PTP, RADIUS, RTPS, SFTP, SMTP, SNMP, SSH, SSL, TCP, Telnet, TLS, TTL, others (SSDP and SIP as well as custom protocols and WebSockets)

FIGURE 2 Sales, Professional Services, And Technical Support Staff

Vendor	Sales*	Professional services*	Development/technical*
Akamai Technologies	500-749	100-249	100-249
CenturyLink	1,000+	25-99	25-99
CloudFlare	25-99	100-249	100-249
DOSarrest Internet Security	0-4	0-24	0-24
F5 Networks	500-749	100-249	25-99
Imperva	100-249	25-99	25-99
Level 3 Communications	1,000+	25-99	25-99
Neustar	100-249	0-24	25-99
Verisign	25-99	25-99	25-99
	*Forrester estimates	*Forrester estimates	*Forrester estimates

FIGURE 3 Service Provider Partners

Vendor	System integration	Technology	Value added resellers
Akamai Technologies	**North America** IBM, Trace 3, HP, Accenture, Novacoast **Western Europe** ITWay Solutions, Schuberg Philis BV, HP Enterprises, CapGemini, Onsight Solutions **Eastern Europe** HP Enterprises, IBM, Security Innovation **Latin America** Edge Technology, IBM, Accenture, HP, Novacoast **Asia North** Zero One Technology, NEC Solution, Innovators, Fujitsu Limited, AT&T, KT Corporation **Asia South** eGuardian Pte, Dimension Data Australia, Joint Force Technology, Centre for Development of Advanced Computing	**Prolexic** Internally developed **KSD** Internally developed, but Akamai Technologies uses certificate authority from other vendors when customers purchase the SSL option. Supported CA include Symantec, CyberTrust, and Comodo	**North America** AT&T, DLT Solutions, LLC, Level 3 Communications, Carahsoft Technology, CGI Technologies **Western Europe** British Telecommunications, BT GmBH, Telefonica Soluciones de Informatica y Comunicacions, Host Europe Solutions GmbH, Milloh CS **Eastern Europe** AddPro, British Telecom, Innovative Solutions, GTS CE, Onsight Solutions **Latin America** Exceda, Digital Media Technologies, AT&T, Novacoast **Asia North** Zero One Technology, Wangsu Science & Technology, Beijing UniNetech, AT&T, TIS **Asia South** 02 Networks Pty, Singtel Telecommunications, AT&T, Microware, Centre for Development of Advanced Computing

FIGURE 3 Service Provider Partners (Cont.)

Vendor	System integration	Technology	Value added resellers
CenturyLink	**North America** Not published	Arbor, Cisco (Arbor), Imperva (Web Application Firewall Service), Juniper (Webscreen Systems)	**North America** Not published **Western Europe** None **Eastern Europe** None **Latin America** None **Asia North** None **Asia South** None
CloudFlare	**North America** Rackspace, Acquia, Spark::red, BlueHost, DreamHost **Western Europe** I-Kos/Inviqa, Blue-Leaf, Realise, 1&1, Bloom **Eastern Europe** Google, Microsoft, Rackspace, IBM, British Telecom **Latin America** Cable & Wireless Panama, Neosecure (Chile), ITG Solutions (Peru) **Asia North** Master Concept **Asia South** British Telecom, Ace Pacific, Haylix, Catalyst.net.nz	Internally developed	**North America** Google, Microsoft, Rackspace, IBM, Acquia **Western Europe** Google, Microsoft, Rackspace, IBM, Capside **Eastern Europe** Google, Microsoft, Rackspace, IBM, British Telecom **Latin America** Google, Microsoft, Rackspace, IBM, Onistec **Asia North** Google, Microsoft, Rackspace, IBM **Asia South** Google, Microsoft, Rackspace, IBM, Ace Pacific

FIGURE 3 Service Provider Partners (Cont.)

Vendor	System integration	Technology	Value added resellers
DOSarrest Internet Security	None	Internally developed	**North America** Tenzing, INetU, DataPipe, HOSTING.com, Acquia **Western Europe** Pulsant **Eastern Europe** Google, Microsoft, Rackspace, IBM, British Telecom **Latin America** None **Asia North** None **Asia South** Batelco, CHJ Technologies Singapore
F5 Networks	**North America** Worldwide Technology, CDW, Optiv, Milestone Systems, Presidio **Western Europe** HP, Dimension Data, Computacenter, NTT Comm Security, Telindus **Eastern Europe** Santa Monica Networks, IBS, S&T, Actinet, IBM **Latin America** CYLK IT Solutions, Agility Networks, Netful, Promon, Novared **Asia North** Global Technology Integrator, Dimension Data, 3D Networks Singapore, B&D Technology, NTT-AT **Asia South** Peering One, Trends and Technologies, Telstra, NCS Pte, IBM	Arbor and internally developed	**North America** Google, Microsoft, Rackspace, IBM, Acquia **Western Europe** Google, Microsoft, Rackspace, IBM, Capside **Eastern Europe** Google, Microsoft, Rackspace, IBM, British Telecom **Latin America** Google, Microsoft, Rackspace, IBM, Onistec **Asia North** Google, Microsoft, Rackspace, IBM **Asia South** Google, Microsoft, Rackspace, IBM, Ace Pacific

FIGURE 3 Service Provider Partners (Cont.)

Vendor	System integration	Technology	Value added resellers
Imperva	**North America** Rackspace Hosting, Accenture, DataPipe, Verizon, Windstream **Western Europe** Accenture, Atos, Telecom Italia, Zion Security, Aiuken Solutions **Eastern Europe** ProtoServices, PostCy Data Center, Clico, DNS a.s., Manta Systems d.o.o. **Latin America** Telefonica, Site Blindado S.A, KorSoftCorp, Scitum, Cipher **Asia North** ProtoServices, LLC, PostCy Data Center, Clico, DNS a.s., Manta Systems d.o.o. **Asia South** SoftBank, NRI Secure Tech, Asgent, Matrix CloudZone, Real Commerce	Internally developed	**North America** Optiv, ePlus, Dunbar Digital, Westcon **Western Europe** Atos, HP Security, Telecom Italia, Exclusive Networks, Evry **Eastern Europe** ProtoServices, PostCy Data Center, Clico, DNS a.s., Manta Systems d.o.o. **Latin America** Telefonica, Site Blindado S.A, KorSoftCorp, Scitum, Cipher **Asia North** SoftBank, NRI Secure Tech, Asgent, Matrix CloudZone, Real Commerce **Asia South** Dimension Data, M. Tech, Evvo Labs, Neto E-commerce solutions, Minjar Cloud Solutions Pvt

FIGURE 3 Service Provider Partners (Cont.)

Vendor	System integration	Technology	Value added resellers
Level 3 Communications	**North America** Akamai/Prolexic*, Neustarr* **Western Europe** None **Eastern Europe** None **Latin America** None **Asia North** None **Asia South** None *Level 3 provides DDoS mitigation service using its own infrastructure and SOC. It also utilizes partners including Prolexic and, in limited cases, Neustar.	Arbor, Juniper Webscreen Systems, Juniper peering and edge routers other: Level 3, Radware, Alcatel Lucent	**North America** Akamai/Prolexic*, Neustarr* **Western Europe** None **Eastern Europe** None **Latin America** None **Asia North** None **Asia South** None *Level 3 provides DDoS mitigation service using its own infrastructure and SOC. It also utilizes partners including Prolexic and, in limited cases, Neustar.
Neustar	None	Arbor, Juniper (Webscreen Systems), other: Citrix, HP	None
Verisign	**Western Europe** KPN International, Deloitte **Asia North** Hitachi Information Systems **Asia South** CSC Global/MBIT	Arbor, Juniper (Webscreen Systems), Verisign, Internally developed	**North America** CSC Global, Analyze Corporation, Internap, Virtual Armor, Juniper Networks **Western Europe** KPN International, Axians (formerly Imtech ICT), Deloitte, Hardware.com **Eastern Europe** None **Latin America** TechBiz Forense Digital LTDA **Asia North** Hitachi Information Systems, ST Electronics (Info-Comm Systems) Pte **Asia South** Distribution Central

DDoS Service Provider Evaluation Overview

For this report, Forrester evaluated the strengths and weaknesses of top DDoS protection service providers to see how they stack up against our criteria and against each other.

The Evaluation Criteria Include Current Offering, Strategy, And Market Presence

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation 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 DDoS product offering. The sets of capabilities evaluated in this category are: the vendor's business description, alert notification process (DDoS monitoring service), amplification attack defense, attack types defended, automated response capabilities (on-demand modes of operation), customer portal features, customer references, data/scrubbing center geographic presence, defended network protocols, defense tactics (prior to an attack), detection tactics, filtering rule deployment times, IP location and maps, response tactics (after an attack is detected), SSL traffic inspection capabilities, standard mitigation times, supported devices, and traffic redirection techniques (see Figure 4).
- **Strategy.** A vendor's position on the horizontal axis indicates the strength of its DDoS strategy, specifically focused on the customer communications process. Solution development plans, business and technical value, pricing models, geographies served, hybrid implementation availability, threat intelligence capabilities, system integration partners, technology partners, value-added resellers, technical and development staff, professional services staff, and sales staff.
- **Market presence.** The size of the vendor's bubble on the chart indicates its market presence, which Forrester measured based on the company's client base, revenue, revenue growth, and the years the firm has offered DDoS services.

Inclusion Criteria Looked At Breadth, Global Presence, And Market Relevance

Forrester included nine vendors in this DDoS assessment: Akamai Technologies, CenturyLink, CloudFlare, DOSarrest Internet Security, F5 Networks, Imperva, Level 3 Communications, Neustar, and Verisign. Each of these vendors has (see Figure 5):

- **A complete suite of DDoS security services.** We included providers that offer a complete suite of DDoS services including both on-demand and always-on modes of operation. DDoS protection services block attempts to render computer resources (e.g., websites, email services, VoIP, or whole networks) unavailable to users.

- **A strong DDoS presence in North America and globally.** To be included, a significant portion of the vendor's DDoS service revenue had to come from clients in North America; however, we also considered Europe and Asia in our inclusion criteria. Many large companies are participants in this Forrester Wave, but we focused only on their DDoS services business.
- **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 Wave.
- **A large installed base of DDoS customers.** The vendor needed to demonstrate a large installed base of DDoS customers with a large part their business revenue from DDoS protection services.

FIGURE 4 Geographic Presence

Vendor	Data/scrubbing center geographic presence
Akamai Technologies	**North America (2)** Prolexic: Ashburn, VA (US), San Jose, CA (US) KSD: Not disclosed **Western Europe (2)** Prolexic: London (UK), Frankfurt (DE) KSD: Not disclosed **Asia North (2)** Prolexic: Hong Kong (CN), Tokyo (JP) KSD: Not disclosed **Asia South (1)** Prolexic: Sydney (AU) KSD: Not disclosed
CenturyLink	**North America (4)** Los Angeles, CA (US), Sunnyvale, CA, (US), Dallas, TX, (US), Washington, DC, US (2) **Western Europe (3)** London, (UK) (2), Frankfurt (DE) **Asia North (1)** Tokyo, (JP)
CloudFlare	**North America (10)** Seattle, WA (US), San Jose, CA (US), Los Angeles, CA (US), Dallas, TX (US), Chicago, IL (US), Atlanta, GA (US), Miami, FL (US), Ashburn, VA (US), Newark, NJ (US), Toronto (Canada) **Western Europe (9)** Paris (FR), Frankfurt (DE), Stockholm (SE), Vienna (AT), Madrid, (ES), Milan, (IT), — Dusseldorf, (DE), London, (UK), Amsterdam, (NL) Eastern Europe (2) Warsaw, (PL), Prague, (CZ) **Latin America (6)** Santiago (CL), Lima (PE), Medellin, (CO), Sao Paulo (BR), Buenos Aires, (AR), Valparaiso, (CL) **Asia North (11)** Hong Kong (CN), Tokyo (JP), Seoul (KR), Qingdao (CN), Fuzhou (CN), Hengyang (CN), Dongguan (CN), Shenyang (CN), Luoyang (CN), Hangzhou (CN), Tianjing (CN) **Asia South (2)** Singapore (SG), Sydney, (AU)
DOSarrest Internet Security	**North America (2)** Locations not disclosed **Western Europe (1)** Location not disclosed **Asia South (1)** Location not disclosed

FIGURE 4 Geographic Presence (Cont.)

Vendor	Data/scrubbing center geographic presence
F5 Networks	**North America (2)** San Jose, CA (US), Ashburn, VA (US) **Western Europe (1)** Frankfurt (DE) **Asia South (1)** Singapore (SG)
Imperva	**North America (10)** Seattle, WA (US), San Jose, CA (US), Los Angeles, CA (US), Dallas, TX (US), Chicago, IL (US), New York, NY (US), Ashburn, VA (US), Atlanta, GA (US), Miami, FL (US), Toronto, Ontario (CA) **Western Europe (7)** London (UK), Paris (FR), Zurich (CH), Frankfurt (DE), Stockholm (SE), Amsterdam (NL), Madrid (ES) **Eastern Europe (1)** Warsaw (PL) **Latin America (1)** Sao Pallo (BR) **Asia North (2)** Hong Kong, (CN) Tokyo (JP) **Asia South (3)** Singapore (SI), Sydney (AU), Auckland (NZ)
Level 3 Communications	**North America (5)** Los Angeles, CA (US), Chicago IL, (US), New York, NY (US), Washington, D.C. (US), Dallas, TX (US) **Western Europe (2)** London (UK), Frankfurt (DE)
Neustar	**North America (2)** Sterling, VA (US), Ashburn, VA (US) **Western Europe (1)** Amsterdam (NL) **Asia South (1)** Singapore (SI)
Verisign	**North America (2)** Ashburn, VA (US), San Jose, CA (US) **Western Europe (2)** Amsterdam (NL), Frankfurt (DE) **Asia North (1)** Tokyo (JP)

FIGURE 5 Evaluated Vendors: Vendor Information And Selection Criteria

Vendor	Product evaluated	Version release date
Akamai Technologies	Kona Site Defender and Prolexic Routed	Kona Site Defender 4.0 and Prolexic Routed 1.0
CenturyLink	CenturyLink DDoS mitigation service (legacy Qwest) and CenturyLink Technology Solutions DDoS mitigation service 2.0 (legacy Savvis)	Legacy Savvis 2.0
CloudFlare	CloudFlare	CloudFlare (security features): CloudFlare DDoS mitigation, CloudFlare web application
DOSarrest Internet Security	DOSarrest Security Services	3.2.2
F5 Networks	F5 Silverline DDoS Protection	F5 Silverline DDoS protection
Imperva	Incapsula DDoS Protection	N/A
Level 3 Communications	Level 3 DDoS Mitigation	N/A
Neustar	SiteProtect	N/A
Verisign	Verisign DDoS services	Verisign open hybrid

Vendor selection criteria

A complete suite of DDoS security services. We included providers that offer a complete suite of DDoS services including both on-demand and always-on modes of operation. DDoS protection services block attempts to render computer resources (e.g., websites, email services, VoIP, or whole networks) unavailable to users.
A strong DDoS presence in North America and globally. To be included, a significant portion of the vendor's DDoS service revenue had to come from clients in North America; however, we also considered Europe and Asia in our inclusion criteria. Many large companies are participants in this Forrester Wave, but we focused only on their DDoS services business.
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 DDoS customers. The vendor needed to demonstrate a large installed base of DDoS customers with a large part of their business revenue from DDoS protection services.

Evaluation Analysis

Each of the DDoS service providers reviewed for this research has the capabilities to become a client's strategic partner. We saw parity across many of the evaluated categories; the Leaders and Strong Performers were close in their scoring.

Each vendor has built a program to address different sized customers. Some (Akamai Technologies, CenturyLink, Neustar, Level 3 Communications, and Verisign) clearly focus on enterprise clients, others (DOSarrest Internet Security and F5 networks) focus on SMB clients, while others (CloudFlare and Imperva) are adept at serving both enterprise and SMB clients.

The average score for customer references in this Forrester Wave was a 3.22. This indicates that all of the customers felt their vendors did an adequate job but did not delight them. Some customers cited cost, others time for deployment, as reasons for not being totally satisfied.

The evaluation uncovered a market in which (see Figure 6):

- **Akamai Technologies, CloudFlare, Imperva, CenturyLink, and Verisign are Leaders.** To be a leader in a Forrester Wave, a vendor must have a strong current offering and a strong strategy that will clearly address current and future market needs. These vendors demonstrate effective portals, good client and revenue growth, and a focus on customer service. Each of the Leaders offers a robust set of capabilities for DDoS protection services, with the ability to defend against the largest amplification attacks and the most pernicious application attacks.
- **F5 Networks, Neustar, DOSarrest, and Level 3 Communications are Strong Performers.** Strong Performers offer solid DDoS protection services and often compete successfully with similar levels of service and price as the Leaders. Compared with the Leaders, the Strong Performers did not rate as consistently well across key areas such as business value, client references, customer services, information portals, security analytics, and threat intelligence. While not all of their capabilities are at the level of the Leaders, if you are looking to outsource security to a competent partner, you should consider these vendors.
- **Nonparticipant vendors Nexusguard, Radware, and Tata Communications can play.** Not all vendors can be formal participants in the Forrester Wave. However, through the course of preparing this research, Forrester spoke with three additional vendors that have DDoS protection services worth considering.

This evaluation of the DDoS protection services market is a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs using the Forrester Wave Excel-based vendor comparison tool.

FIGURE 6 Forrester Wave™: DDoS Services Providers, Q3 '15

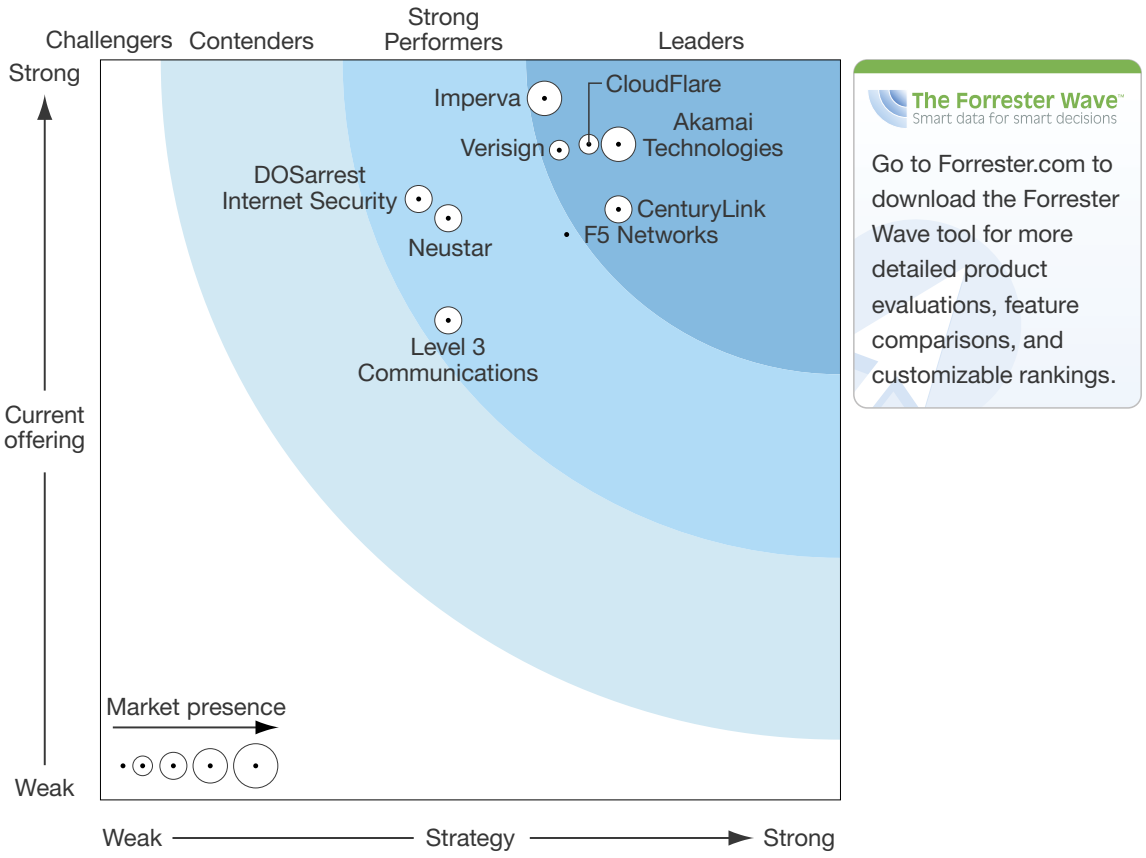

FIGURE 6 Forrester Wave™: DDoS Services Providers, Q3 '15 (Cont.)

	Forrester's weighting	Akamai Technologies	CenturyLink	CloudFlare	DOSarrest Internet Security	F5 Networks	Imperva	Level 3 Communications	Neustar	Verisign
CURRENT OFFERING	50%	4.48	3.99	4.43	4.06	3.82	4.74	3.24	3.93	4.39
Vendor's business description	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Alert notification process (DDoS monitoring service)	5%	5.00	5.00	2.00	5.00	4.00	5.00	1.00	3.00	5.00
Amplification attack defense	7%	5.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00	5.00
Attack types defended	5%	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
Automated response (on-demand modes of operation)	5%	4.00	4.00	3.00	4.00	2.00	5.00	3.00	3.00	4.00
Customer portal	15%	5.00	4.00	5.00	4.00	4.00	5.00	5.00	3.00	5.00
Customer references	10%	3.00	3.00	4.00	3.00	3.00	4.00	2.00	4.00	3.00
Data/scrubbing center Geographic presence	5%	4.00	3.00	5.00	3.00	3.00	5.00	2.00	3.00	3.00
Defended network protocols	2%	5.00	5.00	0.00	0.00	2.00	5.00	3.00	5.00	5.00
Defense tactics (prior to an attack)	2%	3.00	4.00	2.00	4.00	2.00	4.00	2.00	4.00	4.00
Detection tactics	10%	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
Filtering rules deployment	4%	3.00	3.00	5.00	5.00	3.00	5.00	4.00	4.00	3.00
IP location data and maps	3%	5.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Response tactics (after the attack is detected)	7%	5.00	5.00	5.00	4.00	4.00	3.00	3.00	5.00	5.00
SSL traffic inspection	10%	5.00	3.00	5.00	4.00	4.00	5.00	0.00	3.00	5.00
Standard mitigation times	5%	4.00	3.00	5.00	5.00	3.00	5.00	4.00	4.00	3.00
Supported devices	5%	4.00	4.00	5.00	2.00	5.00	5.00	4.00	5.00	5.00
Traffic redirection techniques	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

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

FIGURE 6 Forrester Wave™: DDoS Services Providers, Q3 '15 (Cont.)

	Forrester's weighting	Akamai Technologies	CenturyLink	CloudFlare	DOSarrest Internet Security	F5 Networks	Imperva	Level 3 Communications	Neustar	Verisign
STRATEGY	50%	3.50	3.50	3.30	2.15	3.15	3.00	2.35	2.35	3.10
Customer communication process	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Development plans	10%	5.00	5.00	3.00	4.00	5.00	5.00	3.00	3.00	5.00
Value — business value	10%	5.00	3.00	4.00	3.00	3.00	4.00	1.00	2.00	3.00
Value — technical value	15%	4.00	5.00	5.00	5.00	4.00	4.00	4.00	4.00	5.00
Flexible pricing models	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Geographies currently served	10%	5.00	5.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00
Hybrid implementation	10%	2.00	5.00	5.00	0.00	3.00	3.00	0.00	2.00	2.00
Partners — system integration	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Partners — technology	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Partners — value-added reseller	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Staff — development/technical	15%	2.00	1.00	2.00	0.00	1.00	1.00	1.00	1.00	1.00
Staff — professional services	15%	2.00	1.00	2.00	0.00	2.00	1.00	1.00	0.00	1.00
Staff — sales	5%	4.00	5.00	1.00	0.00	4.00	2.00	5.00	2.00	1.00
Threat intelligence	10%	4.00	4.00	2.00	2.00	3.00	3.00	3.00	4.00	5.00
MARKET PRESENCE	0%	4.00	3.00	2.00	2.50	0.75	3.75	2.75	3.00	1.50
Annual DDoS revenue (Forrester estimate)	25%	3.00	1.00	0.00	0.00	0.00	2.00	2.00	2.00	0.00
DDoS revenue growth (Forrester estimate)	25%	5.00	4.00	0.00	3.00	1.00	5.00	1.00	5.00	0.00
Number of customers using volumetric and Web application defense services	25%	3.00	2.00	5.00	2.00	1.00	5.00	3.00	2.00	2.00
Years offering DDoS defense services	25%	5.00	5.00	3.00	5.00	1.00	3.00	5.00	3.00	4.00

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

Vendor Profiles

Leaders

- **Akamai Technologies is one of the largest CDNs operating globally.** The company provides cloud-based web performance, media delivery, networking, and security solutions. Due to the strong relationship between the company's content delivery network (CDN) business and its DDoS business, Akamai/Prolexic is one of the largest of the DDoS service providers reviewed. Perhaps due to its size, the company showed some rigidity in the way it sells and deploys DDoS services. The company offers two DDoS solutions: Kona Site and DDoS Defender (KSD) and Prolexic Connect and Prolexic Routed.[2] Akamai Technologies' DDoS solutions have significant scale with 15 TBps to 18 TBps of average daily traffic and 26+ TBps in record traffic. Akamai Technologies' platform has more than 8 TBps to 10 TBps of available network capacity, on average.[3] If choosing Akamai Technologies as a vendor for DDoS services, customers should understand there is an overlap of functionality between the two solution stacks. Overall, Akamai Technologies' customers rated the company's DDoS protection services as average. Security and risk pros looking for a large CDN with a significant global DDoS capability should consider Akamai Technologies.
- **CloudFlare provides a content delivery network that includes DDoS services.** The company has excellent capabilities to deliver hybrid DDoS solutions, and its global presence is very strong, including the broad geographic presence of its data/scrubbing centers. CloudFlare boasted fast mitigation times, and customers gave it high marks for service delivery. However, customers also said that customer service could be more responsive. CloudFlare's road map includes extending its relatively low number of network protocols defended as well as expansion of its capabilities in China, improved overall capacity, more third-party integrations, and additional security services.
- **Imperva delivers cloud-based security and DDoS services.** The company has a relatively small staff but a strong global presence and a very large customer base. Customer references had overall positive feedback, and they agreed that the company has strong customer service capabilities and responds well to feedback. Imperva stood out for its SSL traffic inspection and earned strong scores for its IP location maps and network protocols defended. The company's road map plans include extended scope of customer support, enhanced performance, and improvements in analytics. The company has a large global customer base and more than four years of experience delivering DDoS protection services.
- **CenturyLink is a broad-based global communications and services company.** The company offers hosting, cloud, and information technology (IT) as well as DDoS protection services. The company has a relatively small staff and limited partner network, but its global presence is substantial. CenturyLink scored especially well for its attack detection and attack response capabilities as well as its capabilities to defend against very large amplification attacks. Customers commented that they are looking for more from the product road map, but the company is very strong with DDoS fundamentals.

› **Verisign is a DNS service provider offering DDoS mitigation.** The company earned top marks for its customer portal as well as its threat intelligence capabilities. It has a fair amount of experience, providing DDoS services for more than six years. Customers gave the company above-average scores for customer service and noted that staff responded well to special requests; however, they also agreed that the pricing might be too high for some prospective customers. Verisign's development plans focus on improved capacity and better integration capabilities.

Strong Performers

› **F5 Networks is an MSSP with broad capabilities, including DDoS.** The company stood out for its notification capabilities as well as its articulation of business value for its clients. F5 Networks is relatively new to the DDoS services market, and clients said they'd like to see it expand its global presence more. Even with a smaller staff, F5 Networks especially pleased clients with its response time. The F5 Networks road map includes improvements to the customer interface as well as advancements in security offerings such as web application, firewall capabilities, and reputation services.

› **Neustar is a major DNS service provider that also offers DDoS protection services.** This is a relatively new market for Neustar, which has been providing DDoS protection for less than four years. However, Forrester estimates that the company's DDoS revenue growth for the past year has been very strong. Neustar's customer feedback was consistently positive, with praise for its service capabilities as well as its customer service. The references explained that they would like to see a more global presence and faster connections between customers and support staff. The company's development plans include expanding its mitigation capacity, strengthening its reporting capabilities, and offering automation features to streamline customers' interaction with the platform.

› **DOSarrest Internet Security is an MSSP, with DDoS as its core service offering.** The company primarily serves medium-to-large eCommerce sites, and it has a strong global presence. Although it has a very small staff compared with its competitors, it's one of the most seasoned vendors in this evaluation, with more than eight years of experience providing DDoS protection. Customer feedback was mixed with regard to the implementation process, but it was consistently strong for the company's core DDoS protection services. The company's road map includes improvements in monitoring, better reporting, and advancement in protection against evolving attack techniques.

› **Level 3 Communications offers telecom and network services DDoS protection.** The company stands out for its tenure in the DDoS market, providing such services for more than eight years. Level 3 Communications also stood out for the breadth of features in its customer portal. Customer feedback highlighted the company's grasp of fundamental DDoS capabilities but also suggested that these services may get lost in the shuffle among so many other business lines. Development plans include enhancements for greater traffic visibility, a wider scope of protection, and larger

capacity. On July 1, Level 3 Communications acquired DDoS mitigation company Black Lotus, which adds additional scrubbing centers to Level 3's portfolio.[4] Note, these new scrubbing centers and any other post-acquisition enhancements are not reflected in this evaluation.

Nonparticipants

- **Nexusguard provides a global DDoS protection service.** Nexusguard has a globally distributed cloud infrastructure, providing 100% availability during a DDoS attack. The company has 1.28 TBps of mitigation capacity as well as globally distributed scrubbing centers in San Jose, California; Los Angeles, California; Miami, Florida; Ashburn, Virginia; London; Hong Kong; Taiwan; and Singapore. The company's technology uses a heuristic approach that accurately identifies benign users and drops malicious ones. Nexusguard also uses a variety of approaches to improve attack traffic detection.
- **Radware offers hybrid DDoS protection services.** Radware's hybrid DDoS attack mitigation service combines technology and service model to harden clients' Internet-facing assets against cyberattacks. The service integrates on-premises detection and mitigation with cloud-based volumetric attack scrubbing with a straightforward pricing model. Radware's focus is on the hybrid defense model because this approach diverts traffic to the Radware scrubbing center only when the customer's Internet connection is about to saturate.
- **Tata Communications offers DDoS protection as part of its global network.** Tata Communications is one of the largest telecommunication providers globally. The company focuses on SLAs as a source of differentiation for its DDoS protection service. The company has regional scrubbing centers in all major geographies, including North America, Europe, and Asia. The company offers four service options: 1) the on-net service, which collects and monitors flow data 24x7 from within the Tata Communications network; 2) the off-net service, which provides the same capability for customers that don't use the Tata Communications network; 3) domain-name-based protection (DNS Reverse Proxy Solution); and 4) an on-premises CPE DDoS mitigation service, for low and slow application layer attacks, that integrates with its cloud offering. The company also offers a hybrid model for companies that want to use Tata Communications for overflow attack traffic.

Supplemental Material

Online Resource

The online version of Figure 6 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of four data sources to assess the strengths and weaknesses of each solution:

- **Hands-on lab evaluations.** Vendors spent one day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology. We evaluated each product using the same scenario(s), creating a level playing field by evaluating every product on the same criteria.
- **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 product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted surveys that three customer references completed and then had reference calls with one of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then 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 document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we 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, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

All of Forrester's research, including Waves, is conducted according to our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] DDoS attacks have grown in frequency and size. In 2005, the largest DDoS attacks were 9 gigabits per second (GBps) growing to 100 GBps by 2010, according to the Arbor Networks Worldwide Infrastructure Security Report. In December 2013, attackers were utilizing Network Time Protocol (NTP) reflection to amplify their DDoS attacks up to 400 GBps. Researchers have also identified an increase in the average attack size. Source: "Verizon Data Breach Investigations Reports," Verizon (http://www.verizonenterprise.com/DBIR/).

[2] In 2014, Akamai Technologies purchased Prolexic, an accomplished DDoS service provider in its own right. Kona Site Defender provides effective web application defense for both application and amplification attacks directed against

web applications. Kona DDoS Defender provides effective defense against all types of amplification attacks. Akamai Technologies' Prolexic Connect service is a DDoS protection service that is available as an always-on or on-demand service. Prolexic Connect uses the Border Gateway Protocol (BGP) to route network and application traffic through Akamai's global scrubbing centers. Prolexic Routed can stop DDoS attacks for entire IP subnets, for hundreds of web and IP-based applications. Similar to Prolexic Connect, Prolexic Routed uses the BGP to route all of an organization's network traffic through Akamai Technologies' global scrubbing centers. Source: Akamai Technologies (https://www.akamai.com/).

[3] The amount of network traffic Akamai Technologies handles on a daily basis is impressive, and the largest volume attacks the company can absorb are equally impressive. It should be noted that based on the data provided by all of the vendors providing responses to the Forrester Wave, the vast majority of attacks are less than 10 GBps, with many substantially less than this.

[4] Source: "Level 3 Acquires DDoS Mitigation Company Black Lotus," Level 3 Communications press release, July 1, 2015 (http://level3.mediaroom.com/2015-07-01-Level-3-Acquires-DDoS-Mitigation-Company-Black-Lotus).

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.