IDC MarketScape

IDC MarketScape: Worldwide DDoS Prevention Solutions 2019 Vendor Assessment

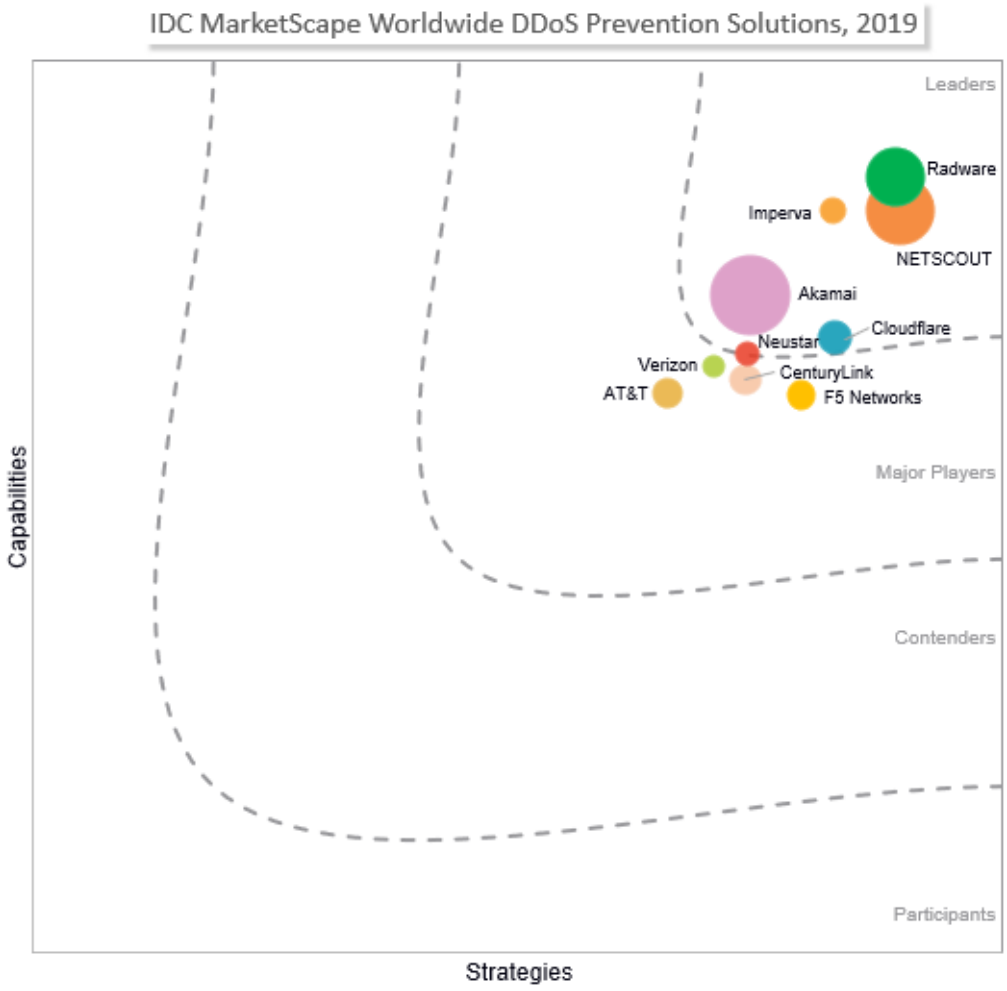
Martha Vazquez

THIS IDC MARKETSCAPE EXCERPT FEATURES CENTURYLINK

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide DDoS Prevention Solutions Vendor Assessment



Source: IDC, 2019

March 2019, IDC #US43699318e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide DDoS Prevention Solutions 2019 Vendor Assessment (Doc #US43699318). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Distributed denial-of-service (DDoS) attacks are increasingly complex, and they frequently employ multiple attack types and strategies such as multivector attacks and diversionary attacks against a broad set of targets. Industry reports continue to illustrate that no one organization is safe. The DDoS attacks that were once solely focused on gaming and retail organizations have spread to target a wide variety of organizations of all sizes and industries. In a 2018 IDC survey, close to half of the respondents said they have experienced a DDoS attack, with over 50% of those organizations experiencing 1–10 times attacks in 2017. Organizations that are experiencing attacks conclude that not only are the attacks volumetric but they experience a combination of multivector, TCP-exhaustion, and/or application attacks.

Even though DDoS prevention solutions are more mainstream solutions than even a few years ago, choosing the right vendor or service is challenging. Organizations have widely varying requirements, requiring all vendors and providers to offer highly customized solutions and extensive support services – which in turn challenges vendors and service providers (SPs) to be highly effective in the management of their resources and to keep prices manageable for the organizations they are defending.

Using the IDC MarketScape model, IDC compared 10 organizations that offer DDoS protection services and solutions and conducted in-depth interviews with these DDoS prevention providers and their customers. Through granular evaluations, IDC found that each provider possesses its owns strengths and weaknesses compared with a peer group, but the clear differences appear in both the current capabilities and future strategies. IDC believes that the following areas will drive the DDoS prevention market forward while providing vendors with the opportunity to hone a differentiated proposition:

- Provide advanced value-added features and capabilities such as real-time monitoring, threat intelligence, web application firewall (WAF), advanced analytics, forensics, proactive management, automation detection and mitigation, SSL traffic inspection, IP protection and cloud signaling techniques.
- Demonstrate pricing models that are flexible for the customer.
- Ensure flexible deployment options that work for the organization, which can provide a cloud-based approach, on-premises, or a combination of both such as the hybrid approach, which includes an integrated approach to sending traffic to the cloud either automatically or upon alert when the on-premises resources are exhausted.
- Provide scalable visibility and DDoS mitigation scrubbing capacity across the globe.

- Offer superior SLAs that provide quick and effective detection and mitigation capabilities.
- Provide customer portal and reporting capabilities.
- Demonstrate quick onboarding methods.
- Provide expertise, support, and experience.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 10 DDoS prevention vendors and providers within the 2019 IDC MarketScape for worldwide DDoS prevention solutions vendor assessment. While the market is broad and contains a variety of players in the market, IDC narrowed the field of participants for this study based on the following criteria:

- **Revenue.** Must consist of discrete DDoS revenue of at least $25+ million in services globally and $12 million for appliance vendors for 2017
- **Geographic presence:** Had to consist of a global footprint with presence in multiple geographies
- **Services/product**. Had to consist of a full DDoS prevention and mitigation solution
- **Customer base.** Had to have a presence in the enterprise segment, with at least 100+ customers

ADVICE FOR TECHNOLOGY BUYERS

Organizations looking to conduct a thorough evaluation of DDoS prevention products and services face a daunting task. The marketplace is composed of vendors that sell on-premises DDoS prevention products or cloud-based services. Some of the included vendors are considered managed security service providers (SPs) that are managing products/cloud-based service, but they also include their own people, process, and procedure for mitigating DDoS attacks. IDC looks at the market from two angles, the products and services, and has seen the services market achieve higher growth, meaning that cloud-based service is becoming a very popular way to deploy DDoS prevention.

Managed security SPs are gaining momentum in this space because of their focus on these areas and because of the predictable operation expense they offer to the buyer through managed services.

But in the DDoS prevention market, partnerships are important, and managed security SPs will have to partner with vendors to provide DDoS prevention and mitigation to their own infrastructure and will then resell their services with their own intellectual property (IP) embedded, and in addition, managed security SPs can also integrate a hybrid approach with product DDoS vendors.

Other cloud-based players in the market have established their IP service and deliver that as a cloud-based service. In any case, when an organization is evaluating and choosing a provider or vendor, it's important to have the following key buying considerations in mind:

- **Review advanced features and capabilities.** With DDoS attacks rising in frequency and volume, product vendors, cloud providers, content delivery network (CDN) providers, managed security SPs, and internet service providers are gaining more interest and creating their own blend of DDoS mitigations. As a result, these providers and vendors continue to add more features and functionality into DDoS prevention solutions. DDoS prevention product companies have taken notice of the need for more extensibility and have adapted solutions to

provide more scalability, features, and functionality into their products. Vendors also continue to add features such as threat intelligence (their own and the ability to integrate with third parties) advanced analytics, machine learning and advanced reporting, and automation capabilities. According to an IDC survey, respondents noted that the top 4 most important features for DDoS protection are real-time monitoring, integration of threat intelligence and advanced analytics, proactive management, and automated detection and mitigation. Vendors and providers are adding additional capabilities and services such as bot management, WAF, IPV6 support, cloud workload protection, SSL, and hybrid techniques (cloud signaling) to enhance visibility and strengthen their capabilities.

- **Review global footprint.** One important aspect for buyers to review when looking for a DDoS vendor or provider is the number of scrubbing centers, security operations centers (SOCs), and capacity offered. Network capacity is the amount of total network bandwidth, and scrubbing capacity is the bandwidth that is dedicated to cleaning the DDoS traffic. It is also important to look at the total infrastructure, which includes the number of SOCs and datacenters that are dispersed globally. Those that are more globally spread out can handle more capacity and mitigate attacks quickly and effectively. The different providers can use various tools and methods to enhance their technique as well. Utilizing providers with a large global network and a large network footprint can provide benefits as those providers are able to mitigate the attacks closer to the source and do this without affecting performance.
- **Evaluate investments in automation detection and mitigation techniques.** Organizations should evaluate vendors and providers that are continuing to investment in automating SOC tools, methods, and techniques that will reduce detection and mitigation time frames. DDoS attacks are the new norm, and as a result, vendors or providers should offer services that will enhance their alert and mitigation capabilities. Some of these vendors are also investing in advanced techniques that will enhance their ability around analysis such as behavioral DDoS detection and mitigation.
- **Review deployment options and hybrid capabilities.** Vendors and providers can provide DDoS protection in a number of ways such as cloud based, on-premises (dedicated DDoS products), or hybrid (see the Market Definition section). Depending on their needs, it is important for organizations to look at flexible deployment options. Organizations need to look at what skills they possess internally today and analyze the number, volume, and source of attacks occurring in order to determine the best way to protect themselves. Some enterprises that are receiving DDoS attacks frequently and are at a higher risk may choose an on-premises product as they are constantly monitoring traffic, and therefore, the product can mitigate attacks before they hit any important parts of the IT infrastructure. However, organizations are also choosing hybrid capabilities, which combines on-premises with cloud-based DDoS prevention service. This provides the organization help defending against larger attacks as well as giving them the opportunity to stop attacks from reaching the network. Cloud signaling is a seamless capability that sends an alert to allow for traffic to be mitigated if the on-premises resources become exhausted. Another deployment capability is only cloud based, which provides monitoring and mitigation via the provider's SOC and scrubbing centers. Organizations can benefit from this option for easier deployment, and the provider can see the traffic occurring on the network and mitigate the bad traffic quickly. In addition, because of their scalability, these types of cloud-based providers can also handle large volumetric attacks.
- **Evaluate portals.** Enhancing the customer experience is important, and so organizations should evaluate user interface, dashboards for ease of use, visibility, and reporting. Vendors are providing features such as real-time monitoring, analytics and graphs, reporting, email reports, traffic usage, incidents, and sources of attacks as well as some self-service capabilities. Some vendors will provide ways to change settings, review statistics, and

examine emerging attacks in real time or see attack history data. The attack history is important as clients are able to see behavior network patterns and show peaks over a period of time. Tracking of tickets and custom centralized reporting to provide visibility to the customer are also some key features of the portal that should be evaluated as well. Buyers should take consideration as to the valuable features that are offered in the portal and test navigation and functionality tools required for their business needs.

- **Investigate pricing options.** Pricing for DDoS protection varies widely across the board, but IDC found that many vendors are increasingly providing flexible pricing options to customers in order to address the widest range of customer requirements. Pricing should be easy to understand and simplified for the customer. DDoS prevention can be priced in a number of different ways such as usage based, consumption based, or based around clean traffic or legitimate traffic and by footprint of assets such as IPs, website, circuit, datacenters, per incident, or per volume. Some vendors are also offering pay as you grow and unmetered pricing options. Enterprises should consider pricing that includes overage charges if attack size becomes too big for the package service purchased. Typically, services that are offered "always on" may be priced higher than those offered on demand, but depending on the customer's risk, an always-on option may fit best for them. Other factors to consider include managed versus self-service as well as integration and set up support services.
- **Review SLAs.** Time to alert, detect, and mitigate is a crucial component to review. Forward-thinking DDoS providers and vendors are looking at different tools and technologies to enhance their monitoring, detection, alerting, and mitigation efforts. Some DDoS vendors can offer very granular and detailed SLAs with specific commitments to mitigation and quality.
- **Consider security expertise and reputation.** Buyers should consider the reputation and security expertise of the vendor or provider that they choose. As early as the onboarding process, it becomes crucial to understand how proficient the vendor guides the customer through the sales to the onboarding process and then throughout the customer life cycle. Buyers should evaluate reputation, longevity, and expertise that providers have in the space and then also evaluate how much support buyers will want from providers' team of experts once the solution is implemented. Buyers should also consider the number of staff that is dedicated to only DDoS in the SOC. In addition, buyers should also look at how these providers are investing in their team of experts through training and retention methods.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

CenturyLink

CenturyLink is positioned as a Major Player in the 2019 IDC MarketScape for worldwide DDoS prevention solutions vendor assessment.

CenturyLink is a global managed security SP that provides a comprehensive security services portfolio to enterprises and governments. CenturyLink provides organizations a multilayered DDoS mitigation approach, which contains threat intelligence and data correlation to detect different types of DDoS attacks. CenturyLink's DDoS Mitigation Service is global with 11 scrubbing centers, located in North America, Europe, Latin America, and Asia/Pacific. CenturyLink provides 43Tbps+ of mitigation capacity using Border Gateway Protocol (BGP) Flowspec and has 4Tbps+ of scrubbing center

mitigation capacity. CenturyLink's global internet backbone allows the company to mitigate against various types of DDoS attacks regardless of the size.

CenturyLink has DDoS mitigation offerings for medium-sized to large enterprises and has a breadth of experience proving to governments globally. These companies can mix and match options for individualized service models for any carrier as well. According to CenturyLink, the company has a number of other differentiators in the market, which include the ability to provide flexible dynamic routing features, unique advantages of IPVPN traffic return, and full mitigation support for Layer 3/4 and Layer 7, and also provides SSL key sharing options for real-time decryption.

CenturyLink's DDoS mitigation services supports customers of any carrier where traffic can be pulled through route redirection (BGP or DNS redirect) and sent to a scrubbing center for mitigation and cleaning. For routed (BGP), customers can choose service types such as on demand, always on, or always routed (auto-mitigation). The solution provides a private connection for forwarding clean traffic, and customers can also choose to have flow-based monitoring added, which provides proactive monitoring and alerting. Customers choosing basic network protection receive BGP route filtering, null routing, transit interface protection, and SOC-triggered and customer-initiated destination-based blackholing. Hybrid offerings are also offered for customers that prefer to have an on-premises solution and then use cloud signaling to CenturyLink's cloud-based service.

Strengths

CenturyLink has a solid security service portfolio, and its DDoS services provides a number of features such as integration of threat intelligence, advanced analytics, and forensics and supports multi-carrier circuits. Customers have a variety of options around how clean traffic is delivered.

CenturyLink expanded its detection by adding flow-based monitoring so customers can see what is occurring directly on their network. The company's threat intelligence, backed by its Threat Research Labs, can track command and control DDoS attacks.

CenturyLink also offers flexible and simple pricing options that are not based on attack size or frequency.

Challenges

CenturyLink is well-known for servicing government and large enterprises versus downstreaming to smaller to midsize organizations.

Consider CenturyLink When

Enterprises and governments entities should consider CenturyLink if they are looking for a provider that has managed security services, cloud-based security services, and/or hybrid capabilities.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the

company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable the vendor to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

A simplistic distributed denial-of-service (DDoS) attack uses a botnet (a group of computers and internet connections) and DNS queries or other means to forward malicious communications to other computers on a network. When the website and/or the network shut down due to the flood of incoming messages, service is denied. The attack often begins when a single computer system is vulnerable and becomes infected. This computer becomes the botmaster who spreads malware and initiates the attack against the target. A denial-of-service (DoS) attack typically involves a single computer and single internet connection.

The DDoS prevention market is composed of a variety of competitors such as internet service providers; managed security (SPs) such as AT&T, CenturyLink, and Verizon; cloud-based providers/CDN or hosting providers such as Akamai, Cloudflare, Imperva, and Neustar; and appliance vendors such as NETSCOUT, F5 Networks, and Radware.

LEARN MORE

Related Research

- *Market Analysis Perspective: Worldwide Managed Security Services Providers, 2018* (IDC #US44316818, September 2018)
- *Worldwide DDoS Prevention Products and Services Forecast, 2018-2022* (IDC #US43994318, July 2018)
- *DDoS Protection Is Now a Necessity and Still Growing: U.S. DDoS Prevention Survey, 2018* (IDC #US43904418, June 2018)

Synopsis

This IDC study presents a vendor assessment of providers offering DDoS prevention and mitigation products and services through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for DDoS prevention. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the DDoS prevention market over the short term and the long term.

"DDoS vendors continue to improve their protection platforms, adding more features and lowering prices to address all segments of the market. As a result, DDoS is more accessible to companies than ever before. However, many vendors warn that the attack sizes and complexities of the past two years are just the beginning. DDoS prevention solutions are a necessity, but the market is competitive, and it is difficult for buyers to choose the right one for them. Buyers need to research and review the competitive features and services provided by each provider and choose the one that best fits their needs," says Martha Vazquez, senior research analyst, Infrastructure Services.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com