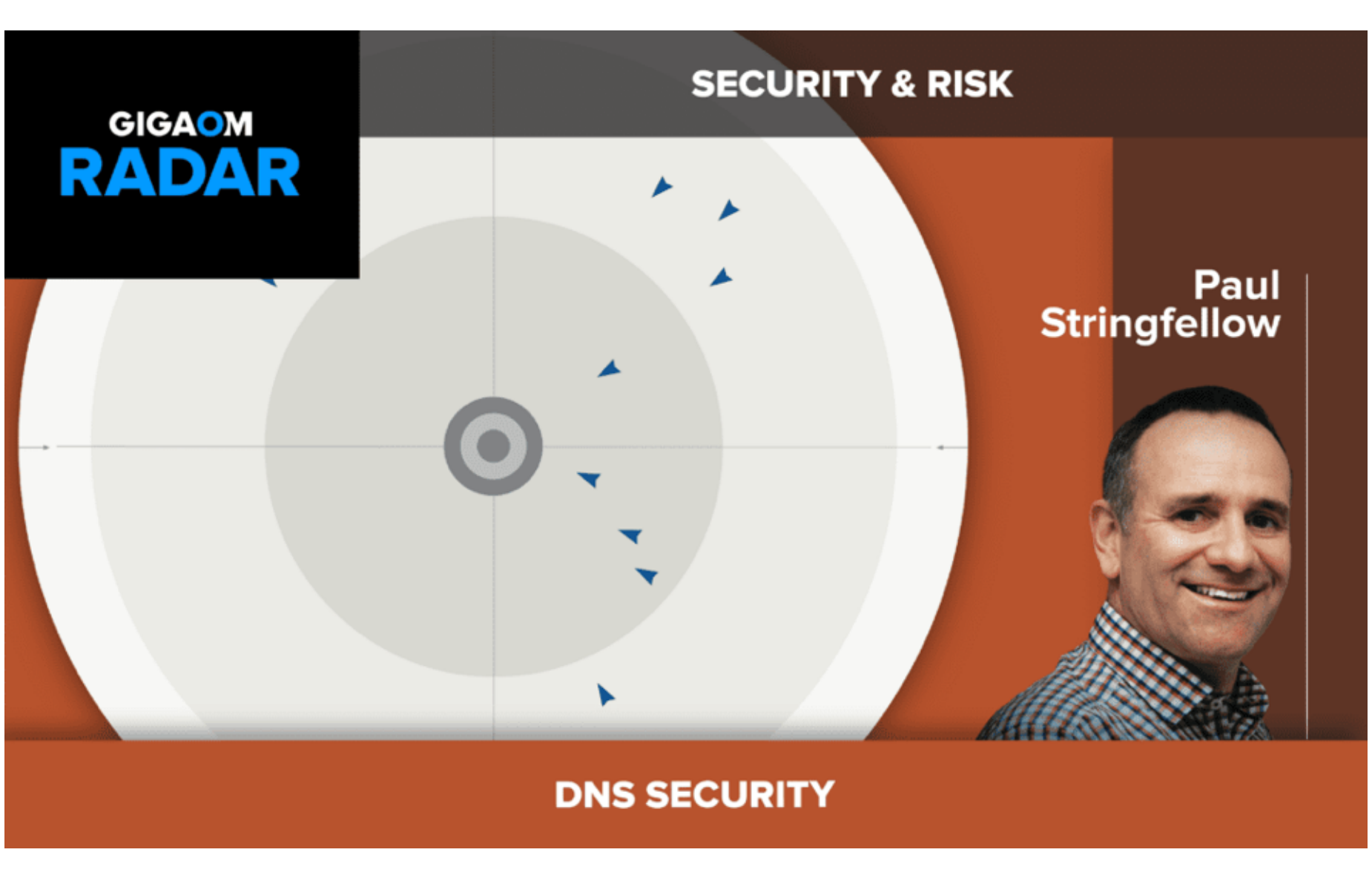
GIGAOM
This GigaOm Research Reprint Expires Mar 1, 2025
Feedback



Paul Stringfellow
Feb 29, 2024

GigaOm Radar for Domain Name System (DNS) Security v2.0

Table of Contents

1. Executive Summary
2. Market Categories and Deployment Types
3. Decision Criteria Comparison
4. GigaOm Radar
5. Solution Insights
6. Analyst's Outlook
7. Methodology
8. About Paul Stringfellow
9. About GigaOm
10. Copyright

1. Executive Summary

The domain name system (DNS) is fundamental to every modern organization. It's the backbone of communications and the means by which clients connect with services both internally and externally. It is a service so fundamental to the basic day-to-day operations of every network that it must be both ultra-secure and resilient. However, the reality is that it is not. In fact, the DNS is vulnerable. Attacks of all types that can undermine the DNS, such as cache poisoning, DNS hijacking, amplification, spoofing, and tunneling, continue to increase.

The impact of a DNS cyberattack on an enterprise can be devastating. It can result in the loss of sensitive data, deployment of malicious code, and denial of access to key services, all of which can result in significant financial losses and reputational damage. Protecting DNS should be a priority, and that means using a solution with a range of security capabilities. A good DNS security solution has a unique value in the overall security chain. This stems from its operation early in the communications process. The vast majority of malicious activity in an infrastructure will make a DNS call; by securing and identifying malicious calls at inception, proactive security can be implemented from the beginning of an attack, helping secure an organization more effectively.

The information gained from a DNS security solution can also greatly enhance an organization's risk analysis and threat response, providing a rich source of data for security teams and improving resilience, availability, and operational stability.

DNS security is often overlooked, as it lacks the high profile of other security threat vectors. However, DNS communication is a fundamental part of IT infrastructure and very few systems and organizations can operate without it. Safeguarding it should be an essential part of an organization's security planning, and the right solution will improve the security of DNS as well as deliver improvements across the broader stack. DNS security has the potential to provide a strong return on investment and should be part of every organization's security strategy.

This is our second year evaluating the DNS security space in the context of our Key Criteria and Radar reports. This report builds on our previous analysis and considers how the market has evolved over the last year.

For this evaluation, we've updated our inclusion criteria to only include vendors that provide DNS security as a discrete service. The DNS security must be a standalone offering, either a specific solution or, if part of a broader portfolio, able to be deployed and licensed on its own, without the need to include other services. This ruled out some vendors we had included previously that only offered DNS security as part of firewalls or secure internet gateways where DNS could not be unbundled. Additionally, we're not including vendors that offer authoritative DNS solutions, where it's required that a user's DNS infrastructure moves to the vendor's platform. This is a separate area of DNS security and needs to be evaluated as such. Instead, this report focuses on solutions that offer DNS security for DNS resolution and client end use and those that provide security to DNS infrastructure. The idea is to ensure greater consistency among vendors and to make comparison easier. Despite the elimination of some vendors, the changes resulted in an increase in the number of vendors included in our report.

This GigaOm Radar report examines 11 of the top DNS security solutions and compares offerings against the capabilities (table stakes, key features, and emerging features) and nonfunctional requirements (business criteria) outlined in the companion Key Criteria report. Together, these reports provide an overview of the market, identify leading DNS security offerings, and help decision-makers evaluate these solutions so they can make a more informed investment decision.

GIGAOM KEY CRITERIA AND RADAR REPORTS

The GigaOm Key Criteria report provides a detailed decision framework for IT and executive leadership assessing enterprise technologies. Each report defines relevant functional and nonfunctional aspects of solutions in a sector. The Key Criteria report informs the GigaOm Radar report, which provides a forward-looking assessment of vendor solutions in the sector.

2. Market Categories and Deployment Types

To help prospective customers find the best fit for their use case and business requirements, we assess how well DNS security solutions are designed to serve specific target markets and deployment models (**Table 1**).

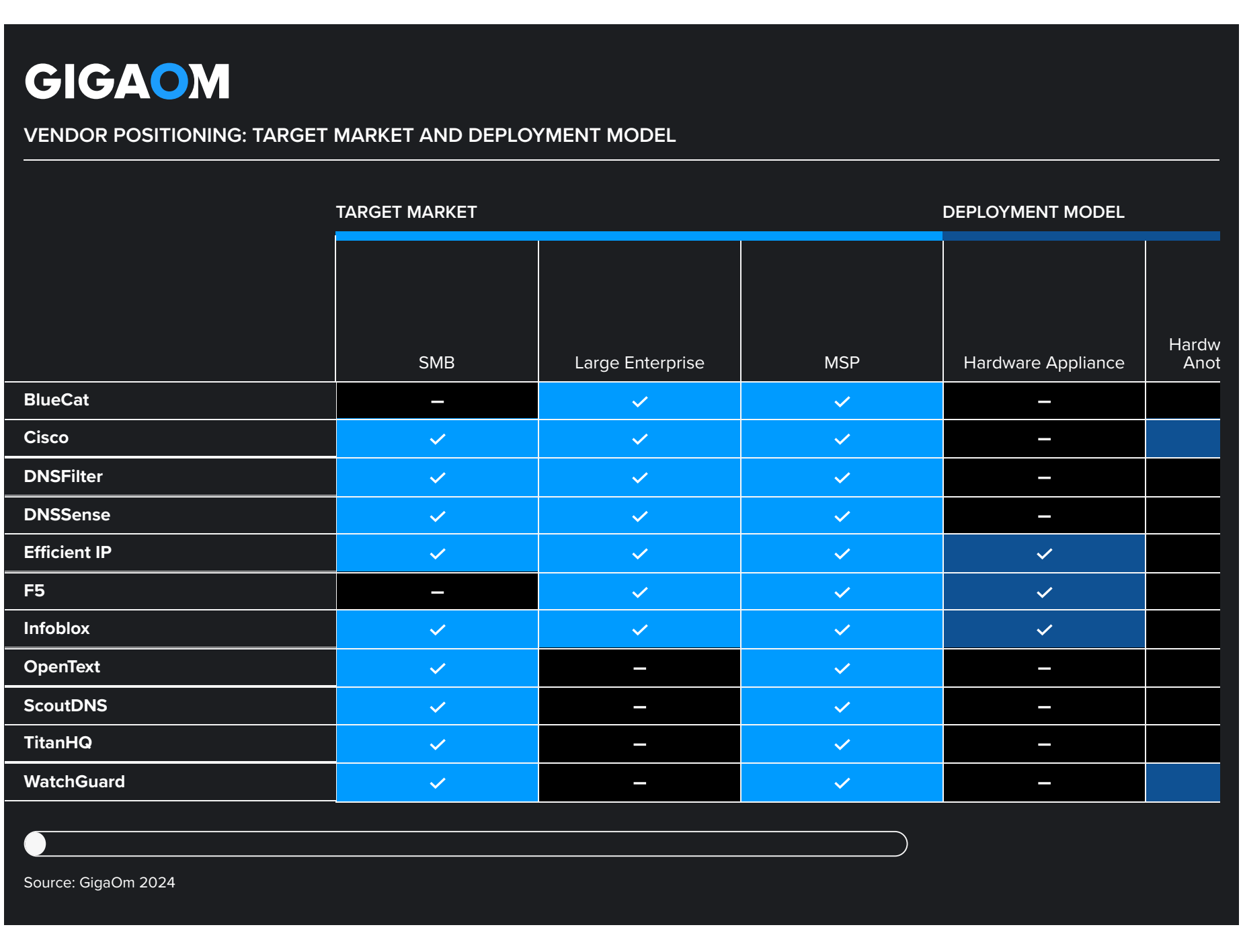
For this report, we recognize the following market segments:

- **Small-to-medium business (SMB):** In this category, we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies. Here, ease of use and deployment are more important than extensive management functionality and feature set.
- **Large enterprise:** Here, offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category have a strong focus on flexibility, performance, scalability, and the ability to effectively integrate into existing environments.
- **Managed service provider (MSP):** Increasingly, organizations across all disciplines of IT are looking to consume managed services to augment in-house capabilities. Here, we assess solutions based on how effective they are in either supporting MSPs, both technically and commercially, or by offering their own managed services.

In addition, we recognize the following deployment models:

- **Hardware appliance:** These solutions are available only as hardware appliances, provided specifically to deliver DNS security. It is acceptable for these devices to provide a broader suite of services such as DDI (DNS, DHCP, and IP management).
- **Hardware as part of another service (for example, a firewall):** These solutions are delivered on a hardware appliance, but in this case, DNS security is part of a broader security suite, such as DNS protection offered as a service on a hardware firewall. To be included in the report, the vendor must also offer the DNS security capability as a standalone service.
- **Software:** The DNS security solution is available as software that can be installed on a standard operating system, either on-premises or on a public or private cloud.
- **Software as a service (SaaS):** These solutions are available only in the cloud, designed, deployed, and managed by the vendor. The advantages of this type of solution are its simplicity, ease and speed of scaling, and flexible licensing models. We recognize that some DNS security solutions may include endpoint agents, so SaaS relates to the way the core administration and management engines are deployed.
- **Cloud native/cloud image**: With these solutions, the primary administration and management engines can be deployed and supported as a public cloud-based service. The main components can be deployed either as a cloud-native service or as a public cloud image, usually, although not exclusively, available from a cloud provider's marketplace. In these instances, they are not shared and are specific to a single customer.

Table 1. Vendor Positioning: Target Market and Deployment Model



GIGAOM
VENDOR POSITIONING: TARGET MARKET AND DEPLOYMENT MODEL

	TARGET MARKET			DEPLOYMENT MODEL
	SMB	Large Enterprise	MSP	Hardware Appliance
BlueCat	–	✓	✓	–
Cisco	✓	✓	✓	–
DNSFilter	✓	✓	✓	–
DNSSense	✓	✓	✓	–
Efficient IP	✓	✓	✓	✓
F5	–	✓	✓	✓
Infoblox	✓	✓	✓	✓
OpenText	✓	–	✓	–
ScoutDNS	✓	–	✓	–
TitanHQ	✓	–	✓	–
WatchGuard	✓	–	✓	–

Source: GigaOm 2024

Table 1 components are evaluated in a binary yes/no manner and do not factor into a vendor's designation as a Leader, Challenger, or Entrant on the Radar chart (**Figure 1**).

"Target market" reflects which use cases each solution is recommended for, not simply whether that group can use it. For example, if an SMB could use a solution but doing so would be cost-prohibitive, that solution would be rated "no" for SMBs.

3. Decision Criteria Comparison

All solutions included in this Radar report meet the following table stakes—capabilities widely adopted and well implemented in the sector:

- Known bad domain blocking
- Content filtering
- Central administration
- Protection against well-known attacks
- DNS traffic reporting

Tables 2, 3, and 4 summarize how each vendor included in this research performs in the areas we consider differentiating and critical in this sector. The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the relevant market space, and gauge the potential impact on the business.

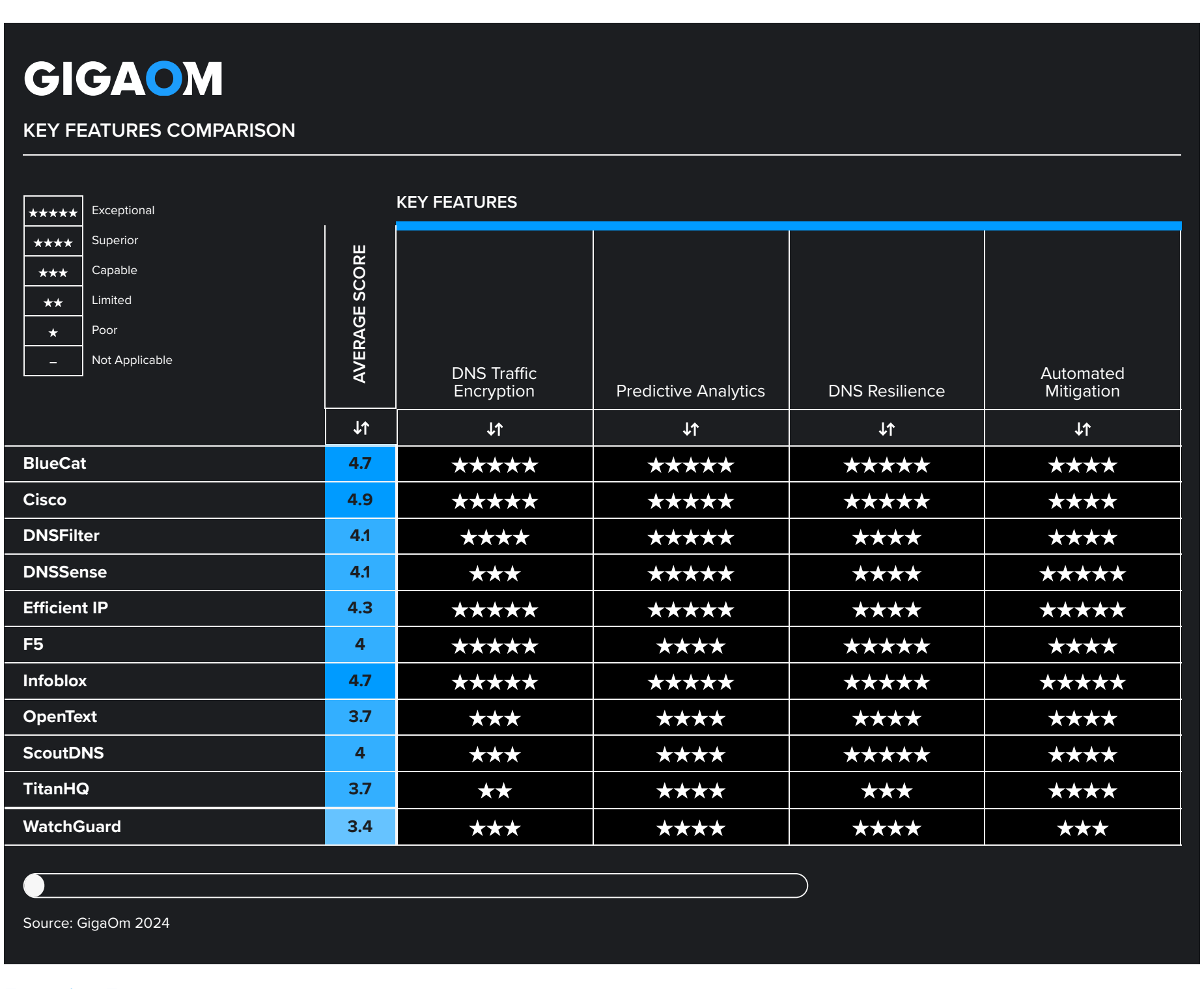
- Key features differentiate solutions, outlining the primary criteria to be considered when evaluating a DNS security solution.
- Emerging features show how well each vendor is implementing capabilities that are not yet mainstream but are expected to become more widespread and compelling within the next 12 to 18 months.
- Business criteria provide insight into the nonfunctional requirements that factor into a purchase decision and determine a solution's impact on an organization.

These decision criteria are summarized below. More detailed descriptions can be found in the corresponding report, "GigaOm Key Criteria for Evaluating DNS Security Solutions."

Key Features

- **DNS traffic encryption:** DNS traffic encryption is both a valuable DNS security tool and a potential attack vector. Effective solutions should be able to use protocols such as DNS over HTTPS (DOH) and DNS over TLS (DoT) to both secure DNS traffic and detect its use, and analyze the traffic for potential threats.
- **Predictive analytics:** The ability to identify DNS threats early is essential to mitigate risk. Strong predictive analytics models can help by identifying actions, like suspicious domain creation, to provide early warnings and enforce protections ahead of attacks.
- **DNS resilience:** DNS is essential to everyday business communications, so ensuring its continuity even in the face of outages or attacks is vital. DNS security solutions must therefore be designed to be equally resilient and allow users to continue to operate even if there are component failures within the solution.
- **Automated mitigation:** Fundamental to cybersecurity defense is a quick response to threats. Automated mitigation, whether done natively in the solution or via third-party integration, significantly improves an organization's ability to respond to threats, reduce risk, and improve security operations.
- **Security stack integration:** DNS security is an essential part of the overall security workflow. Leading solutions should be capable of integrating with an organization's existing tools, such as security information and event management (SIEM), security orchestration, automation, and response (SOAR), service desk, and endpoint management tools, both to ensure full coverage of the security landscape and to ease adoption and implementation.
- **Payload analysis:** DNS traffic can be used as a method of "hiding" other kinds of traffic, so security solutions should analyze DNS traffic and understand its payload. Even valid DNS resolution can direct users to malicious content and payloads, so solutions that can analyze such content either natively or via integration bring additional value to customers.
- **Threat intelligence platform integration:** The use of threat intelligence platforms is increasingly commonplace. These large models that aggregate millions of security metrics deliver more accurate threat analysis and guidance to security enforcement tools. Their use should be an integral part of DNS security solutions, helping to more quickly identify DNS threats.

Table 2. Key Features Comparison



GIGAOM
KEY FEATURES COMPARISON

★★★★★ Exceptional
★★★★ Superior
★★★ Capable
★★ Limited
★ Poor
– Not Applicable

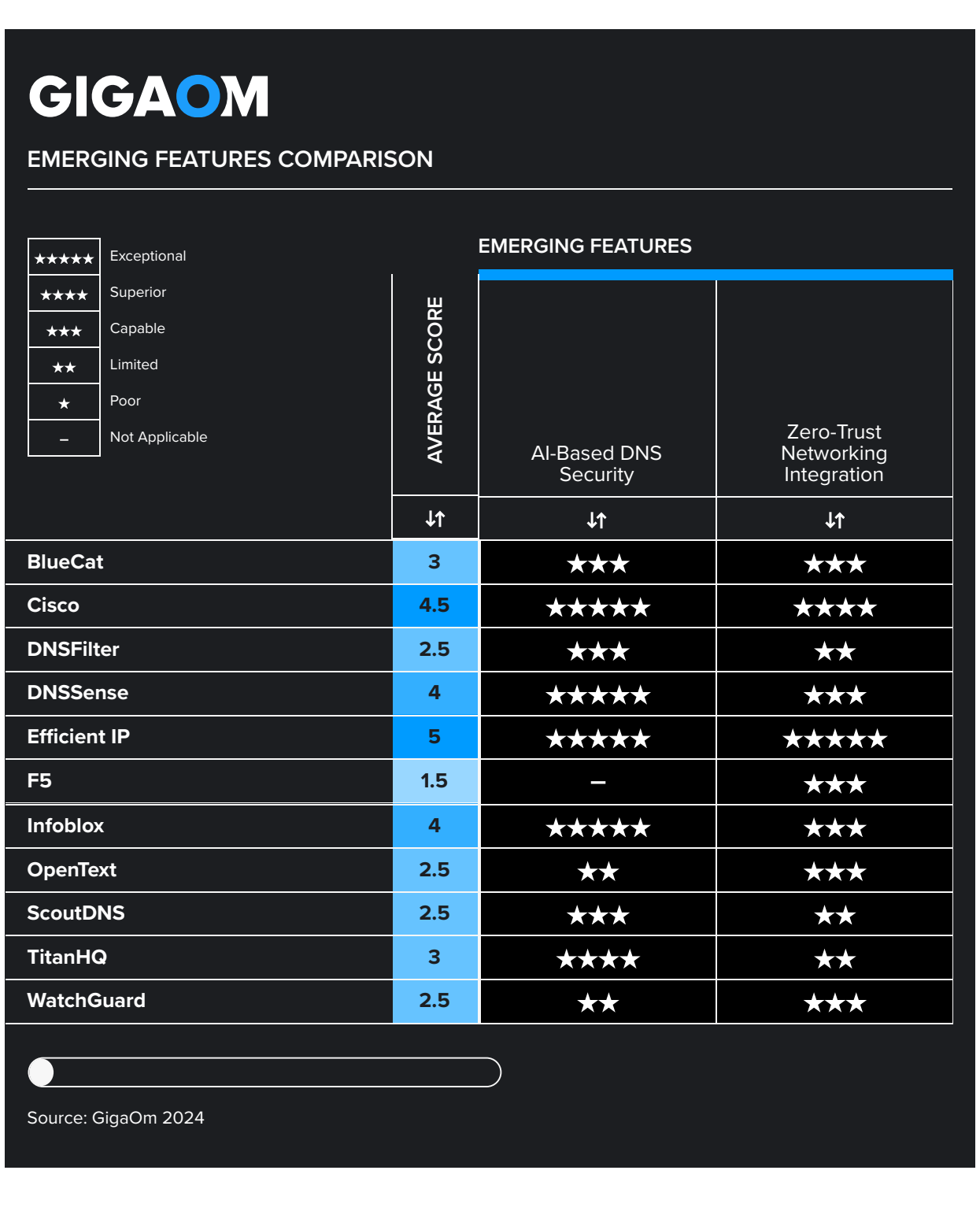
	AVERAGE SCORE	KEY FEATURES			
		DNS Traffic Encryption	Predictive Analytics	DNS Resilience	Automated Mitigation
BlueCat	4.7	★★★★★	★★★★★	★★★★★	★★★★
Cisco	4.9	★★★★★	★★★★★	★★★★★	★★★★
DNSFilter	4.1	★★★★	★★★★★	★★★★	★★★★
DNSSense	4.1	★★★	★★★★★	★★★★	★★★★★
Efficient IP	4.3	★★★★★	★★★★★	★★★★	★★★★★
F5	4	★★★★★	★★★★	★★★★★	★★★★
Infoblox	4.7	★★★★★	★★★★★	★★★★★	★★★★★
OpenText	3.7	★★★	★★★★	★★★★	★★★★
ScoutDNS	4	★★★	★★★★	★★★★★	★★★★
TitanHQ	3.7	★★	★★★★	★★★	★★★★
WatchGuard	3.4	★★★	★★★★	★★★★	★★★

Source: GigaOm 2024

Emerging Features

- **AI-based DNS security:** The use of AI and analytics continues to grow in all aspects of cybersecurity, and we expect leading solutions to increasingly use AI models to help users more effectively identify and mitigate potential DNS threats.
- **Zero-trust network integration:** Zero trust, which involves continuously analyzing user behavior to ensure access privileges remain appropriate, is an important aspect of modern cybersecurity. DNS security solutions can be a part of this by feeding useful metrics to zero-trust tools to help enrich behavioral information. We expect to see this type of integration increasingly within DNS security tools.

Table 3. Emerging Features Comparison



GIGAOM
EMERGING FEATURES COMPARISON

★★★★★ Exceptional
★★★★ Superior
★★★ Capable
★★ Limited
★ Poor
– Not Applicable

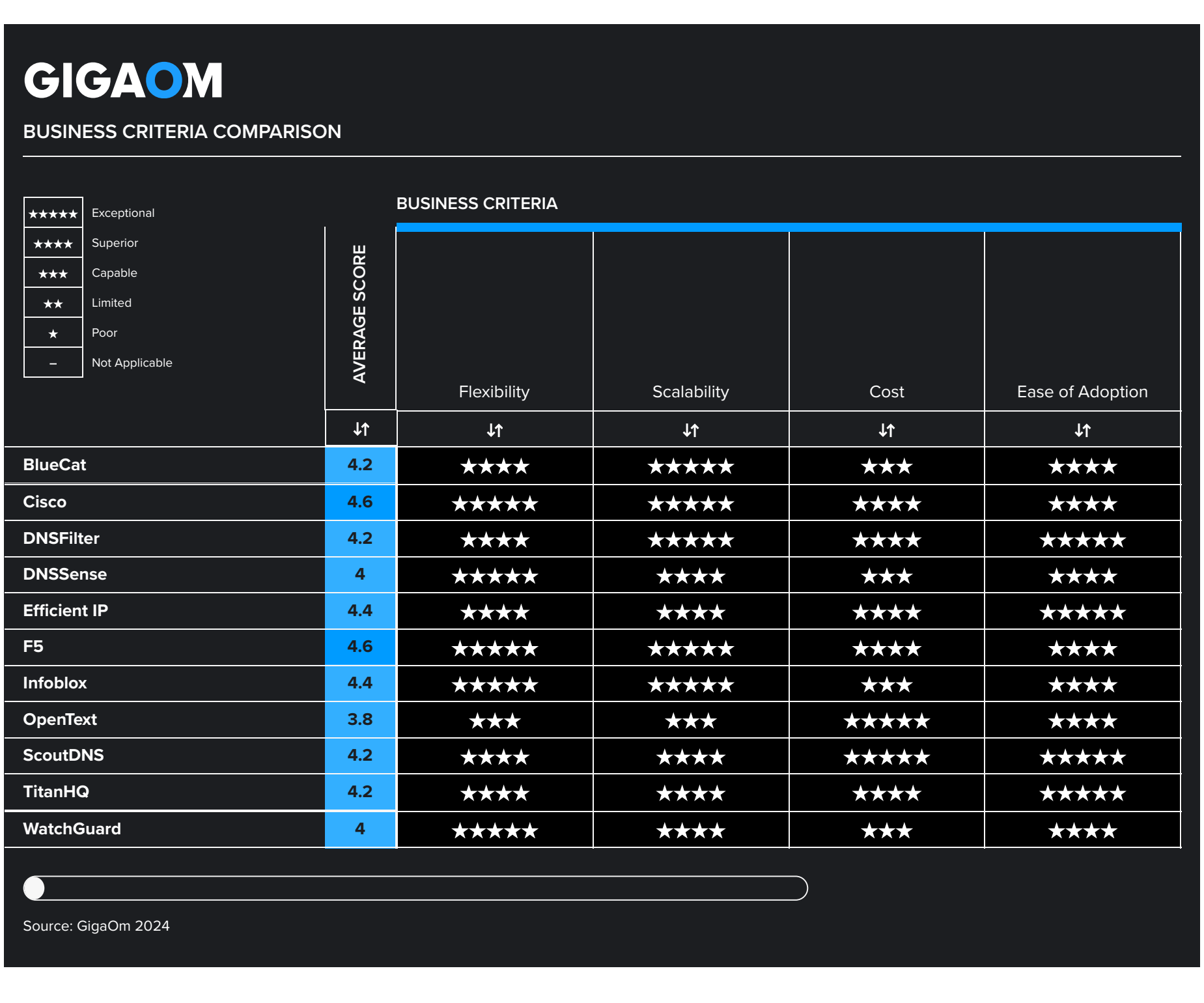
	AVERAGE SCORE	EMERGING FEATURES	
		AI-Based DNS Security	Zero-Trust Networking Integration
BlueCat	3	★★★	★★★
Cisco	4.5	★★★★★	★★★★
DNSFilter	2.5	★★★	★★
DNSSense	4	★★★★★	★★★
Efficient IP	5	★★★★★	★★★★★
F5	1.5	–	★★★
Infoblox	4	★★★★★	★★★
OpenText	2.5	★★	★★★
ScoutDNS	2.5	★★★	★★
TitanHQ	3	★★★★	★★
WatchGuard	2.5	★★	★★★

Source: GigaOm 2024

Business Criteria

- **Flexibility:** Customer environments vary widely and may change over time. Security tools, including those focused on DNS security, must offer different features, deployment models, and adoption techniques to fit a broad range of potential customer needs.
- **Scalability:** The use of DNS is a critical part of modern IT infrastructure. As organizations grow in the number of devices that require DNS resolution, any DNS security solution must be able to scale to continue to meet their needs. Moreover, this scalability should be simple to ensure solutions can grow easily to meet changing demands.
- **Cost:** As with any technology being evaluated, potential buyers of DNS security solutions must understand what the total cost of the investment will be. This includes the price of a license or service as well as its adoption and running costs. Vendors who can show cost efficiency to customers will provide an attractive offering.
- **Ease of adoption:** A DNS security solution is only valuable if adopted across an organization. Customers will be looking for solutions that reduce risk to existing DNS traffic and flows but also are easy to adopt. Solutions that have little impact on or visibility to users are especially useful.
- **Breadth of service offering:** DNS is a core part of IT infrastructure, and finding the right security partner is crucial. Some customers will be looking to also manage adjacent technologies such as IP and DHCP, and solutions that offer these DNS-adjacent services to further improve DNS security will be appealing.

Table 4. Business Criteria Comparison



GIGAOM
BUSINESS CRITERIA COMPARISON

★★★★★ Exceptional
★★★★ Superior
★★★ Capable
★★ Limited
★ Poor
– Not Applicable

	AVERAGE SCORE	BUSINESS CRITERIA			
		Flexibility	Scalability	Cost	Ease of Adoption
BlueCat	4.2	★★★★	★★★★★	★★★	★★★★
Cisco	4.6	★★★★★	★★★★★	★★★★	★★★★
DNSFilter	4.2	★★★★	★★★★★	★★★★	★★★★★
DNSSense	4	★★★★★	★★★★	★★★	★★★★
Efficient IP	4.4	★★★★	★★★★	★★★★	★★★★★
F5	4.6	★★★★★	★★★★★	★★★★	★★★★
Infoblox	4.4	★★★★★	★★★★★	★★★	★★★★
OpenText	3.8	★★★	★★★	★★★★★	★★★★
ScoutDNS	4.2	★★★★	★★★★	★★★★★	★★★★★
TitanHQ	4.2	★★★★	★★★★	★★★★	★★★★★
WatchGuard	4	★★★★★	★★★★	★★★	★★★★

Source: GigaOm 2024

4. GigaOm Radar

The GigaOm Radar plots vendor solutions across a series of concentric rings with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—balancing Maturity versus Innovation and Feature Play versus Platform Play—while providing an arrowhead that projects each solution's evolution over the coming 12 to 18 months.

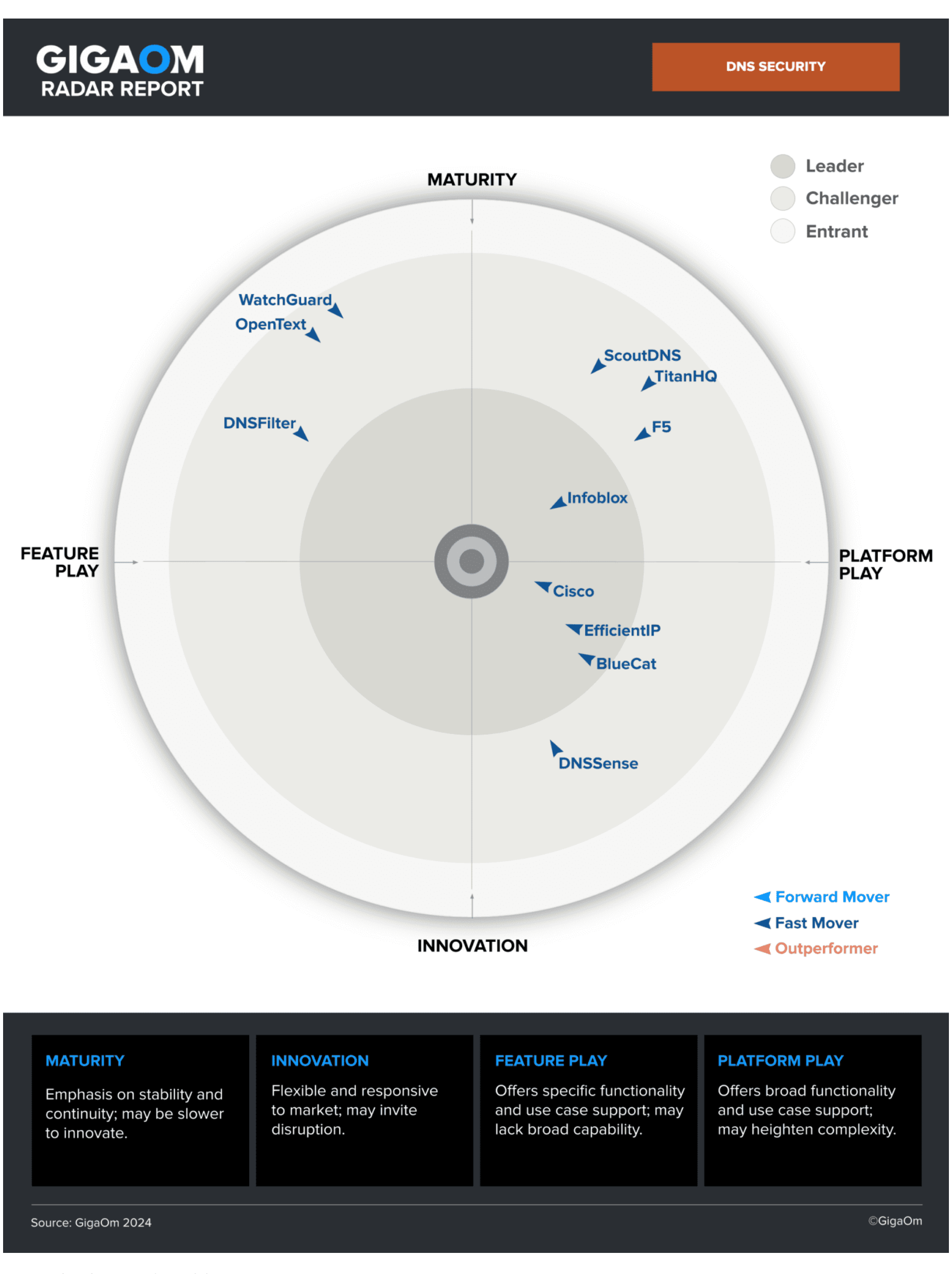


Figure 1. GigaOm Radar for DNS Security

As you can see in the Radar chart in **Figure 1**, the majority of vendors are in the Maturity half. These are players that are generally working on improving existing technologies and finding ways to make DNS security more effective within their current approaches rather than working to develop new features or methods. There are, however, some vendors taking different approaches. These innovative vendors are those showing new deployment options, the smart integration of tools to provide effective DNS, and novel ways of managing existing infrastructure.

The majority of vendors are also on the Platform Play half of the chart. These are vendors that offer a wider range of security tools—in particular, additional security features that apply to DNS—as well as general resolution and communications technologies such as DHCP and IP management. In contrast, the Feature Play vendors are those that focus on DNS protection, usually in the form of filtering. Their solutions often are more straightforward to deploy, are based around category filtering, and don't offer any DNS-adjacent security capabilities, such as DHCP and IP management, traffic proxying, or packet analysis.

The changes in decision criteria and in our scoring system allowed a broader range of vendors in this report, though with fewer in the Leaders circle. Vendors that moved from Leaders to Challengers were mainly impacted by a mix of some new criteria and the more granular scoring system we're now using rather than any diminished quality in vendor solutions.

The Leaders in this report tend to be those that took a more holistic approach to DNS security, often adding additional capabilities, and scored well accordingly. Those that offered strong threat intelligence integration, which can make a significant difference to the efficacy of DNS security, and those that scored well in more complex areas, such as DNS encryption, predictive analytics, and automation, also tended to be leaders. It should be noted, however, that all of our vendors provide strong basic capabilities to enhance DNS security and all have worked hard to ease adoption and ensure a low risk of impact on day-to-day operations.

As the chart shows, we did not see any vendors we felt outperformed their competition in the speed of development, and we found all were continuing to develop their solutions at a steady pace, so we expect a number of the strong Challengers to become Leaders with our next refresh of this report.

Our research showed a set of accomplished vendors offering a wide range of capabilities for users looking to address shortfalls in their DNS security, all providing technologies that continue to improve and will enhance any business's security posture.

In reviewing solutions, it's important to keep in mind that there are no universal "best" or "worst" offerings; there are aspects of every solution that might make it a better or worse fit for specific customer requirements. Prospective customers should consider their current and future needs when comparing solutions and vendor roadmaps.

INSIDE THE GIGAOM RADAR

To create the GigaOm Radar graphic, key features, emerging features, and business criteria are scored and weighted. Key features and business criteria receive the highest weighting and have the most impact on vendor positioning on the Radar graphic. Emerging features receive a lower weighting and have a lower impact on vendor positioning on the Radar graphic. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and roadmaps.

Note that the Radar is technology-focused, and business considerations such as vendor market share, customer share, spend, recency or longevity in the market, and so on are not considered in our evaluations. As such, these factors do not impact scoring and positioning on the Radar graphic.

For more information, please visit our Methodology.

5. Solution Insights

BlueCat: DNS Edge

Solution Overview
BlueCat Networks develops innovative, software-centric solutions enabling automated, centralized, scalable, and secure IP infrastructure, including a full DDI solution. For this report, however, we're evaluating DNS Edge, BlueCat's standalone DNS security solution.

DNS Edge is a SaaS-based solution with a management plane consisting of two parts. The first is a cloud instance, which is the central analytics, policy management, and logging platform. The second, service points, can be installed as on-premises physical appliances, virtual machines, or in AWS or Azure as a service. They act as a DNS caching layer that is deployed between client devices and upstream DNS infrastructure, providing visibility and control of DNS traffic, along with policy enforcement. This infrastructure is deployed on-network but does not require any configuration of endpoints. Queries are directed to service points, which evaluate the query against current policies, threat intelligence sources, and other factors. Based on the evaluation, service points can take actions to mitigate threats, and they can also act as a local DNS cache, which can speed up response time.

The solution is simple to deploy with some minor reconfiguration of DNS information for clients, with no need for agents. It has a central admin console to simplify operations, and its cloud-based design makes it scalable and resilient, including geographic region failover. The solution can also provide branch DDI services for remote offices. For Cisco Umbrella users, there is a specific integration with DNS Edge Identity service. This allows it to collect User Principal Name (UPN) information by parsing directory event logs stored in an Azure Event Hub and embed it in extension mechanisms for DNS (EDNS) in queries forwarded to Cisco Umbrella for processing. This allows it to enforce user or group policies on queries.

Strengths
Areas where BlueCat is particularly strong include:

- **Security stack integration:** In addition to BlueCat's own broader portfolio, DNS Edge integrates well with the other security tools, thanks to its extensive APIs and also to well-established integrations with Cisco Umbrella and CrowdStrike, which enrich the solution with capabilities that enable threat intelligence, zero trust, content filtering, and more.
- **DNS traffic encryption:** DNS Edge offers comprehensive DNS traffic encryption capabilities. It allows customers to block DoH/DoT for further investigation. It has the ability to use DNS over TLS to secure communications, as well as native DNSSEC support to ensure DNS requests are protected from things such as cache poisoning.
- **Scalability:** DNS Edge's cloud-based core management engine, with its service point design flexibility, provides a solution that can scale easily to support large and complex network environments.

Challenges
Areas for improvement include:

- **Off-network coverage:** With no client agent or service, protecting clients off-network can be more difficult. DNS policy and configuration could be used to enforce connectivity, but this lacks the control or insights an endpoint agent would provide.
- **Complexity:** While the platform is relatively easy to adopt, customers should be aware it will require planning and some expertise to ensure service points are configured properly and deployed in the correct locations. This may make it less suitable for smaller companies.

Purchase Considerations
BlueCat's comprehensive analytics of DNS traffic is likely to require more experienced security personnel to take advantage of the information provided. Customers should consider the skills and experience of their internal staff and the additional education that might be required if the solution is adopted.

Common use cases include those seeking a standalone DNS security solution that can be deployed within their network rather than a complete DDI portfolio, and MSPs looking for the same to offer to customers.

Radar Chart Overview
BlueCat's strong performance across all of our technical and business criteria positioned it as a Leader in this report. Its breadth of support for DNS security capabilities and its innovative approach to deployment (SaaS only) placed it in the Innovation/Platform Play quadrant.

Cisco: Cisco Umbrella

Solution Overview
Cisco offers a comprehensive suite of security solutions to service customers from small businesses to the largest enterprises. Cisco Umbrella is a cloud-based security service edge (SSE) solution with platform optional software-defined wide area network (SD-WAN) integration for secure access service edge (SASE) that brings together multiple security tools into one SaaS-based offering. Umbrella is a global solution designed to operate at scale, with a flexible adoption model to support a wide range of use cases.

Within Umbrella, DNS security is available via the following standalone solutions:

- **Cisco Umbrella DNS Essentials** provides basic DNS threat-blocking capabilities that target malware, botnets, and more. It also offers real-time activity reporting, application discovery, and visibility into DNS traffic.
- **Cisco Umbrella DNS Security Advantage** builds on basic DNS blocking by adding selective web security to provide deeper insights and better control over internet traffic for enhanced risk protection and SSL decryption.
- **Cisco Umbrella SIG Essentials** and **Cisco Umbrella SIG Advantage** offer DNS security plus additional capabilities such as secure web gateway (SWG), AV scanning, malware sandboxing, cloud access security broker (CASB) and data loss prevention (DLP), and remote browser isolation (RBI).

Customers can also upgrade to Cisco Secure Access, which provides the same DNS capability as Cisco Umbrella (using the same DNS resolver architecture) plus additional capabilities such as zero-trust network access (ZTNA) and digital experience monitoring (DEM). This option will be attractive to those looking to build their security capabilities in stages.

As Umbrella is a SaaS platform, adoption is relatively straightforward and provides a range of deployment options. In its simplest form, DNS requests can be forwarded to Umbrella from existing infrastructure. For those with existing Cisco infrastructure, many of its solutions, such as Cisco Meraki networking, Cisco Secure Firewall (ASA and FTD operating systems), and Cisco Integrated Service Routers, all have prebuilt integrations with Umbrella that can be enabled. A number of clients are available for both desktops and mobile devices to support off-network controls.

The solution's controls are integrated with Cisco Talos threat intelligence, which includes both analytics and security experts to ensure that new DNS threats are quickly identified and that the DNS security controls within Umbrella are rapidly updated.

Strengths
Areas where Cisco is particularly strong include:

- **Predictive analytics:** Cisco's Talos threat intelligence gathers a broad array of metrics that are then analyzed and used both by its experts and AI/ML to rapidly identify potential malicious DNS activity and proactively mitigate the threat.
- **Security stack integration:** Umbrella offers a good range of prebuilt integrations as well as comprehensive APIs for custom integrations, allowing it to work seamlessly with any existing security stacks.
- **Flexibility:** As part of a SASE platform, Umbrella offers a broad range of integrations. Users can adopt it solely for its DNS security capabilities but can easily adopt more advanced features with simple license key additions. Its range of implementation options and off-network protection provides the flexibility to meet most use cases.
- **Breadth of service offering:** For many customers, the ability to grow security stacks when needed is attractive. Umbrella's design allows customers to move easily from DNS-only security to more advanced DNS and security features.

Challenges
Areas for improvement include:

- **Cost:** Cisco presents a premium, comprehensive product with a purchase price that is likely to be higher than some DNS security competitors.
- **Support response time:** Smaller organizations sometimes find it difficult to get prompt support responses. This is not unique to Cisco but should be considered when evaluating.

Purchase Considerations
Umbrella DNS Security is a part of a comprehensive SASE platform. While it can be purchased as a standalone DNS security product, customers should evaluate how using it for DNS only compares with purpose-built DNS security tools, from both a technical perspective that assesses our criteria, and a cost perspective, especially if Cisco is not already a part of the environment.

This solution is a good fit for existing Cisco customers looking to enhance DNS security. Umbrella provides an initial step toward enhancing their security stack with DNS security, and it can also help them fulfill a longer-term goal of adopting broad SASE capabilities. It will also serve MSPs looking for a DNS security partner very well.

Radar Chart Overview
Cisco scored extremely well on all of our main technical and business criteria, marking the vendor a Leader. The vendor provides strong DNS security capabilities plus a range of other features to further harden DNS security, and it's positioned in the Innovation/Platform Play quadrant.

DNSFilter

Solution Overview
DNSFilter is a SaaS-based DNS security service that leverages AI/ML to block threats before they can reach devices.

DNSFilter offers a range of setup options, including DNS redirections, a lightweight proxy that can be installed on-site, and a number of endpoint agents for both desktop and mobile clients that extend data protection to off-network devices.

The solution is available in three tiers—Basic, Pro, and Enterprise—with additional premium add-ons available that include enhanced service-level agreements (SLAs) and API integrations. Prices are found on the DNSFilter website.

The solution offers a number of additional capabilities that go beyond simple DNS protection, such as dynamic content filtering powered by its Webshrinker AI platform and app protection controls that include a one-click application filter, AppAware, to help quickly block identified high-risk applications. It also offers protective DNS, public Wi-Fi hotspot protection, and single sign-on integration, and it enables customers to build custom DNS protection rules. It also recently introduced Malicious Domain Protection, which is a new predictive analysis approach that looks to reduce threats by inspecting solely the domain string. This provides protection for customers where there is very little other information about the domain.

DNSFilter offers a simple central management interface that includes detailed and customizable reports. For a simple solution, DNSFilter provides a wide range of capabilities, and its claims of high efficacy are backed by independent tests. This is a simple solution that is easy to try and should prove useful for businesses of all sizes.

Strengths
Areas where DNSFilter is particularly strong include:

- **Ease of adoption:** The solution provides a good range of deployment options, including a useful endpoint client for off-network protection. With a simple setup once integrated into the network and little impact on end users, DNSFilter makes adoption easy for customers.
- **Scalability:** Though DNSFilter is simple, it is cloud-based, giving it the ability to support large and complex networks. It currently supports over 32,000 customers and should be able to grow to meet changing customer needs. It should also be noted from a performance perspective that DNSPerf currently ranks DNSFilter as the fastest DNS resolver on the market when looking at raw performance data.
- **Payload analysis:** DNSFilter offers a range of payload analysis options, including granular filtering and AI-driven threat identification and mitigation. This is essential to ensure that users are not redirected to malicious content even if DNS requests are valid.
- **Predictive analytics:** DNSFilter uses its Webshrinker AI technology to drive accurate content filtering, enabling customers to carry out one-click blocking on potentially malicious sites and applications.

Challenges
Areas for improvement include:

- **Documentation on DNS traffic encryption:** While DNSFilter scored well in this category, it was not immediately clear how the solution helps with securing DNS over an HTTPS connection. Upon further investigation, the vendor clarified that, either via its network relay or Roaming Clients, it encrypts all network and client traffic using DoT. When a DoH browser or connection is identified, it runs the DNS query across DoT instead. This is a complex threat for organizations, and it would be helpful for DNSFilter to make this information easier to find.
- **Support add-ons:** Customers should be aware that to gain both case prioritization and enhanced SLAs, they will be required to purchase add-ons. This is the case even for those with Enterprise licenses.
- **API premium add-on:** A permanent API token to use API integrations with the platform will also need to be purchased separately.

Purchase Considerations
DNSFilter is a straightforward and comprehensive solution that should be easy to adopt. Customers should be aware, however, of the additional costs of adding premium support options and should ensure these are included in overall cost considerations.

This solution is a good fit for those looking for a solution that's simple to adopt and use but still offers comprehensive DNS security and filtering. It's also suitable for those needing DNS security for off-network devices, and MSPs looking for a potential partner.

Radar Chart Overview
DNSFilter takes a filtering protection approach to DNS security and continues to develop its existing tools, positioning it in the Maturity/Platform Play quadrant. The solution scored very well across many of our decision criteria but slightly less well in its use of threat intelligence and in the availability of broader capabilities, positioning it as a strong Challenger just outside of the Leaders circle.

DNSSense: DDR 2.0

Solution Overview
DNSSense is a specialist DNS security company with a portfolio of DNS security-centric solutions, including DNSEye, DNSDome, and Cyber X-Ray, which it brings together in its DNS Detection and Response 2.0 (DDR 2.0) solution. Dome and X-Ray are SaaS-based, while DNSEye is an on-premises virtual appliance that gives detailed insight into all traffic—including DNS—across the enterprise network. Together, these solutions deliver comprehensive DNS security.

Cyber X-Ray operates as an AI-powered domain intelligence solution that provides fast domain classification (typically within a 10-minute window for brand-new domains, which can be blocked until classified as part of security policy). Updates are applied to customers' DNS classifications immediately. It uses this AI capability to also allow it to block previously unknown threats and DNS tunneling attacks

DNSDome is the core DNS security engine that is used to enforce DNS security policy, either automated or custom, through any of the tools available to it. This includes its roaming client, which can be installed on Mac, Windows, and iOS devices for continued DNS protection when off-network.

DNSSense positions itself as complementary rather than a competitor to many of the other vendors that operate in the space, building strong two-way integrations with several endpoint detection and response (EDR) vendors to ensure that detailed DNS activity context is applied. This is an attractive option for those with an existing security stack who are keen to extend their DNS security while maintaining that investment.

Strengths
Areas where DNSSense is particularly strong include:

- **Predictive analytics:** Cyber X-Ray gathers detailed telemetry from devices and across networks, then uses its AI capabilities, extensive analytics, and threat intelligence to more accurately predict DNS threats. This is further enhanced by its ability to integrate with several leading EDR platforms.
- **Automated mitigation:** The solution offers automated mitigation via its DNS detection and response capability as well as its integration with XDR solutions, which enhances its automation capabilities on endpoints. It uses its continuous threat intelligence to update domain classifications and policies to ensure strong protection. Users can build policies for mitigation resolution.
- **Flexibility:** DNSSense is a flexible solution that can meet varied customer needs. With a good range of deployment options, as well as both network analysis and off-network protection, it can cover many use cases. Its ability to integrate with well-established endpoint protection solutions allows customers with these technologies to maintain their investment while augmenting their DNS security capabilities.

Challenges
Areas for improvement include:

- **Support response time:** The vendor admitted that it is still scaling up its support capabilities, which sometimes leads to slow support responses. Customers should evaluate this to ensure that support levels will meet their needs.
- **UI:** The vendor has also acknowledged it would like to improve the user interface to ensure users can more quickly gain value from the product.
- **Customer focus:** This solution is aimed at those with at least 500 devices to be secured. Therefore, it is unlikely to be suitable for smaller customers.

Purchase Considerations
While the three solutions can be purchased individually, all three components are necessary to get the benefit of the full DDR 2.0 approach, and that cost should be considered during evaluation. However, 24/7 support and regular service health check calls are included in the standard product price.

For customers with fewer than 500 users, the solution will have limited value and there may be more suitable alternatives.

Common use cases include midsize and larger businesses that wish to enhance their DNS security, as well as organizations that have invested in existing EDR solutions but need to improve their DNS security. DNSSense's range of integrations makes it a strong contender, particularly for those looking for a DNS security solution that can also analyze local network traffic to provide comprehensive local network protection and for MSPs looking for a DNS security partner.

Radar Chart Overview
DNSSense brings some interesting innovations to the space—including how it uses AI, how it integrates threat intelligence, and its ability to deeply analyze all network traffic to provide additional security and insight—and it's positioned in the Innovation/Platform Play quadrant. In addition, it scored consistently well across our decision criteria, positioning it as a strong Challenger in this report.

EfficientIP: 360° DNS

Solution Overview
EfficientIP is a network automation and security company specializing in DDI solutions. It offers several DNS security tools, including filtering, firewalling, behavioral attack detection, threat intelligence, and threat investigation tools.

For this report, we looked at the 360° DNS security solution, which consists of five products. The SOLIDserver appliance is a DDI solution including a hardened DNS server that can manage existing DNS infrastructure both on-premises and in the cloud. It enforces best practice policies and delivers zero-day protection and DNS firewall capabilities, mixing client and destination in advanced filtering policies. DNS Intelligence Center provides live insights on DNS domains across the internet—it claims global-scale AI-based data collection and analytics, with over 5 million observations per second and 3 billion domain entries that provide rich domain insights. Threat Pulse is a multisource threat intelligence feed, built using AI-powered algorithms to proactively combat threats like domain generation algorithms (DGAs), ransomware, and phishing. These services are underpinned by the DNS Guardian service, which delivers real-time DNS Transaction Inspection (DTI), enabling the identification of even the most advanced attacks, such as data exfiltration, DNS tunneling, and sloth domain attacks. DNS Blast is a purpose-built DNS cache appliance capable of delivering secure DNS at extreme load and providing strong protection against DNS attacks such as denial of service.

This is a comprehensive mix of cloud services and devices that can provide extensive coverage across on-premises, cloud, and hybrid environments. With its impressive ability to manage a broad array of existing DNS servers, it can meet the most complex infrastructure demands.

Strengths
Areas where EfficientIP is particularly strong include:

- **Predictive analytics:** The solution combines DNS analytics, DNS Guardian's advanced threat detection, and its threat intelligence platform to provide comprehensive predictive analytics. The solution's dynamic policy application capabilities act on this information to quickly mitigate risks from current and emerging DNS threats.
- **Automated mitigation:** The solution offers proactive and automated DNS responses across its entire infrastructure. It employs patented adaptive countermeasures, including blocking source IPs, rate limiting DNS traffic, and quarantining suspected IPs. Its intelligent automation hub provides it with a specific DDI automation capability, and it can also integrate with external systems to act as part of a broader enterprise security orchestration approach. Currently, these integrations are facilitated via API or plug-in libraries, with additional purpose-built integrations on the roadmap.
- **Ease of adoption:** Once the 360° DNS components are deployed to gain the full DNS security capability, the solution's ability to manage and monitor a wide array of third-party DNS services will help ease adoption, especially in more complex environments that already have extensive DNS deployments. Managing these existing infrastructures would derisk adoption and lower adoption costs.

Challenges
Areas for improvement include:

- **Complexity:** The full 360° DNS security solution comprises multiple products for licensing purposes only, aiming to provide greater flexibility in addressing customer needs. There is a single software interface through which the customer can activate various security features on demand. The only exception to this is the DNS Intelligence Center, offered as a cloud service and accessible through a simple cloud user interface. However, this range of products can make adoption more complex.
- **Lack of prebuilt integrations:** The solution currently only offers some prebuilt integrations, including Cisco Umbrella, Tufin, Terraform, and Palo Alto. Though the solution has extensive APIs for building custom integrations into the enterprise security stack, the customer experience could be improved by providing a bigger library of prebuilt integrations into leading enterprise tools and applications.

Purchase Considerations
This platform is a DNS-centered security platform composed of multiple solutions. While it adds granularity and flexibility, it can also introduce complexity to the buying process. Customers should fully evaluate the capabilities of each element to ensure that each will be used within the organization and deliver value for its investment.

This solution is well suited to organizations looking to enhance their DNS security by hardening configurations and security on existing DNS infrastructure rather than replacing it or using DNS filtering tools. It could also prove useful to those looking for a single vendor that can provide a comprehensive range of other DNS-related services in addition to DNS security, and to MSPs looking for a DNS security partner.

Radar Chart Overview
360° DNS's broad range of advanced DNS security capabilities, alongside an innovative approach to managing existing infrastructure, positions the vendor in the Innovation/Platform Play quadrant. It scored well across our decision criteria as well, marking it as a Leader in our report.

F5: BIG-IP DNS

Solution Overview
F5 is a well-established vendor that provides services across app and API protection, performance and reliability, traffic management, content delivery, and DNS security, which includes a primary or secondary authoritative DNS service. For this report, we'll look at its BIG-IP DNS solution.

BIG-IP DNS is a comprehensive platform designed to scale DNS queries and responses while also securing both DNS infrastructure and DNS client requests. It can be deployed as a hardware device or as a virtual appliance. Services can also be purchased with DNS load balancing and on-demand scaling, which ensures good application performance for users. The devices can be deployed globally with anycast integration, enabling automated load distribution across the estate.

The solution is also classified as a DNS firewall that can help protect infrastructure from common attacks such as denial of service and cache poisoning. The platform supports DNSSEC signing and validation. The appliances manage and decrypt DNS over HTTPS to provide full DNS traffic validation and inspection of packets for malicious content. It also supports DNS over TLS to ensure secure DNS communications.

The BIG-IP environment can be managed from a single centralized interface, although this currently looks a little dated compared to its competitors. However, it is effective and provides a central location for creating iRules to manage DNS policies. Advanced features such as ZoneRunner can be used to reduce the risk of zone misconfigurations, and DNS health monitoring provides insights into DNS infrastructure service health. The management platform also provides advanced reporting and analytics, targeted to its large enterprise market.

Strengths
Areas where BIG-IP DNS is particularly strong include:

- **DNS traffic encryption:** The solution offers comprehensive capabilities here, including the ability to decrypt DNS over HTTPS to ensure there is no malicious content within encrypted DNS packets. With support for DNS over TLS as well as DNSSEC and DNS firewall capabilities, it provides robust protection of DNS traffic.
- **DNS resilience:** BIG-IP DNS is built for large and complex enterprises, and its products are designed for use in highly resilient deployment models. This includes the ability to build highly available clusters and to deploy these clusters across multiple sites and geographies.
- **Flexibility:** F5 provides a wide range of appliances to meet customer needs depending on the scale of DNS requests to be protected, from approximately 250,000 requests per second on the virtual appliance to more than 6 million requests per second on its more robust hardware. Licensing is also flexible, with models that include subscriptions as well as the ability to "spin up" or "spin down" services as needed.

Challenges
Areas for improvement include:

- **Payload analysis:** While the solution provides detailed insights into DNS traffic, it does not offer advanced payload analysis, such as scanning of content on completion of DNS resolution. This isn't necessarily an issue, as it's not what the solution is designed to do. Nevertheless, customers should be aware that alternative controls will be needed.
- **Complexity:** There is inherent complexity in a solution designed to meet the demands of large-scale DNS infrastructure and its security, and this may be exacerbated by the requirement to deploy and configure appliances. Moreover, it doesn't help that the current management GUI looks dated and is due for a refresh.

Purchase Considerations
This is a solution designed for complex DNS environments, and it offers comprehensive capabilities. Those looking only for DNS security must determine whether the additional capabilities would bring value to their organizations.

BIG-IP DNS is suitable for large enterprises looking to secure and optimize their DNS environments. F5 offers a comprehensive suite of capabilities for the most complex environments as well as for those looking for a primarily on-premises DNS security solution.

Radar Chart Overview
F5 offers an established technology that provides a broad range of DNS security capabilities, positioning it in the Maturity/Platform Play quadrant. It scored consistently well across our criteria, positioning it as a strong Challenger.

Infoblox: BloxOne Threat Defense

Solution Overview
Infoblox provides a range of solutions that incorporate automation, networking, and security. Its BloxOne Threat Defense, the focus of this evaluation, uses DNS threat intelligence to detect and block malicious activity related to known, unknown, and zero-day threats, providing strong DNS detection and response.

Infoblox delivers a DNS solution designed to protect DNS communications by detecting and identifying threats and providing automatic responses to them. The solution offers flexible installation options and can be deployed on-premises, in the cloud, and as a hybrid or SaaS solution. Infoblox positions the solution as an XDR platform for DNS and delivers the kind of capabilities that would be expected in XDR. The platform is intended to reduce incident investigation and response time, and streamline threat hunting, threat research, and similar capabilities. It uses automation and ecosystem integrations to improve SecOps efficiency, with integrations for SIEM and SOAR tools as well as firewalls and IT service tools. The solution also offers mobile and desktop clients to extend threat defense off-network, and can easily protect IoT and multicloud environments.

BloxOne exploits Infoblox's extensive threat feeds, including its own established threat intelligence team, to help identify threats early and block them before they become high risk. Its threat intelligence is infrastructure-centric, focusing on identifying attacker infrastructure and monitoring activities as they evolve, thus providing effective predictive blocking of malicious domains before attacks are launched.

Strengths
Areas where BloxOne is particularly strong include:

- **Predictive analytics:** The solution offers extensive analytics capabilities that help customers deal with challenges such as lookalike domains and suspicious domain feeds, providing insight into domains that currently look innocent but could prove malicious in the future. It supports proactive activities for customers via its domain takedown service, allowing customers to report potential threats, which Infoblox then takes preemptive action against.
- **Automated mitigation:** The solution contains its own automation engine. This is enhanced with prebuilt integrations and APIs, enabling integration with SIEM, SOAR, and service desk platforms to help drive operational efficiency.
- **DNS traffic encryption:** BloxOne has the ability to understand DNS traffic and spot malicious activity in encrypted packets and includes support for DoH and DoT in terms of encryption between server and client DNS traffic. DNSSec and DNS firewall are also supported as standard capabilities.
- **Flexibility:** BloxOne has a broad market focus with a wide range of installation options and strong integration with enterprise security tools, enabling it to meet the needs of most potential customers.

Challenges
Areas for improvement include:

- **Alert fatigue:** The vendor indicated that customers continue to list "too many alerts" as one of their top SecOps challenges. A new capability will address this by providing additional context for alerts, including user and device information to help with triage. It will enable more effective prioritization of alerts and provide insights to SecOps on how better to jumpstart investigations on significant events. However, this is still a new service, and its effectiveness in reducing alert fatigue is yet to be fully evaluated.
- **Complexity:** Customers with fewer than 250 users will likely lack the skills to take full advantage of many of the advanced features. This may be addressed in some cases by the company's protective DNS (PDNS) services, but customers with less experienced teams should consider whether Infoblox is suitable.

Purchase Considerations
BloxOne is available in four different packages ranging from Essentials to Advanced, and with licensing options either per device or per user. With its broad range of solutions, it may be more complex than can be handled easily by less experienced SecOps teams. Customers will need to evaluate their environments to determine whether this solution will meet their needs.

This solution is well suited to organizations with complex environments that are looking to add DNS security to protect their on-premises, remote, IoT, and multicloud environments. It should also prove useful to those looking longer term to acquire full DDI capabilities from a single vendor but wish to start with DNS security, to larger organizations requiring an on-premises or hybrid solution, and MSPs looking for a DNS security partner.

Radar Chart Overview
Infoblox offers a comprehensive set of DNS and DNS-adjacent capabilities that it continues to evolve and improve, and it's positioned in the Maturity/Platform Play quadrant. It scored very well across all of our key technical and business criteria, making it a strong Leader.

OpenText: Webroot DNS

Solution Overview
OpenText offers a wide range of IT services for a broad spectrum of customers. Its security division has grown through numerous acquisitions, including Webroot DNS Protection, its SaaS-based DNS filtering solution. Integration into current environments is through the use of DNS resolvers or via deployment of its Windows-based client, which allows customers to have DNS control of off-network devices.

At the core of the solution is OpenText's BrightCloud Threat Intelligence platform, which is used to categorize the domain of each DNS request, with those determined to be malicious rerouted to a block page. BrightCloud offers AI/ML-powered analytics backed by security analyst support to ensure the DNS filtering is quick enough to reduce the risk of zero-day threats, and made more accurate with the help of human intervention.

The solution includes the company's patent-pending DNS leak prevention, which provides a firewall for DNS and can be used to ensure DNS traffic is routed only to DNS sites marked as safe, with any alternate sources of DNS resolution, including encrypted DNS such as DoH and DoT, being blocked.

Strengths
Areas where Webroot DNS Protection is particularly strong include:

- **Threat intelligence:** Its BrightCloud platform provides comprehensive threat intelligence, thanks to its interaction with OpenText's broad security portfolio. This enables the solution to gather large amounts of telemetry, which is used to effectively filter malicious DNS traffic.
- **Cost:** The vendor provides transparent pricing on its website and offers easy-to-access free trials. This will help reduce evaluation costs for customers. Its straightforward deployment model should also help to reduce solution costs.
- **Ease of adoption:** The solution is easy to deploy alongside existing infrastructure, thanks to its broad use of APIs, and deployment has little impact on end users. Configuration is simple, and there is good support and help available freely during installation.

Challenges
Areas for improvement include:

- **macOS support:** The Windows protection client is a valuable feature to help protect off-network devices, but there's no macOS client yet. However, this is on the company's current roadmap.
- **Reporting:** Logging DNS requests results in a significant amount of data. Succinctly reporting on the data and turning it into actionable insights for users is another challenge that needs to be addressed.

Purchase Considerations
Webroot DNS Protection is a simple-to-use and effective product. It is aimed at the SMB market, so users in larger enterprises will need to evaluate whether this product would be suitable. The website provides transparent pricing, and prospective customers can trial the software.

Agent support is Windows only; customers with non-Windows estates looking for off-network support will need to consider other options.

This solution is well suited to SMBs seeking an effective DNS filtering solution, those with Windows environments looking to provide off-network protection, and MSPs looking for a DNS filtering technology partner.

Radar Chart Overview
The solution is built on a good set of existing capabilities to provide a strong DNS filtering capability and is positioned in the Maturity/Feature Play quadrant. It scored well across a number of our criteria, although less well in some of the more advanced areas, marking it as a Challenger.

ScoutDNS

Solution Overview
ScoutDNS is a DNS security solution that offers content filtering and threat protection to block malware, adware, and other threats. It also provides network visibility by aggregating up to 30 days of real-time logs.

The solution is a SaaS application built on a global anycast network. Connectivity to the service is via either network relays or endpoint clients. Implementation is straightforward with single-click installation and central configuration of clients and relay agents. Traffic from the network is rerouted via the DNS relay to the central filtering service. The endpoint client does the same while enabling customers to protect off-network devices.

The solution provides comprehensive DNS protection with a range of analysis and blocking capabilities, including stopping adware and malicious scripts hidden in web code fragments, and blocking domains based on virus threats. These are powerful capabilities to reduce risk on sites where DNS resolution has been allowed. Moreover, ScoutDNS has a strong reporting engine that allows customers to interrogate 30 days' worth of live logs, which provides detailed insight into areas such as RDATA and DNS content and top-level domains.

The solution also offers good customization, allowing users to create custom top-level domain block lists to further reduce organization-specific risks. Web filtering is powered by its AI-based URL filter, which claims over 60 million URL scans daily. All are managed from its central UI.

Strengths
Areas where ScoutDNS is particularly strong include:

- **Payload analysis:** ScoutDNS claims to be the only solution that captures full RDATA on every query and, via its reporting engine, allows admins to inspect any full DNS message payloads seen in the last 30 days. The solution can analyze and process suspect data automatically or allow users to carry out analysis manually.
- **DNS resilience:** ScoutDNS offers strong resilience in service design with its anycast network stretching across multiple data centers and regions. On-premises relays can function in HA clusters, and endpoint clients will fail to open if the service is unavailable.
- **Cost:** The simplicity and ease of adoption of this solution will help to keep adoption costs low. Pricing is clearly visible on its website, and customers can trial the solution easily; this will help to both speed up and reduce the cost of evaluation and adoption.

Challenges
Areas for improvement include:

- **Support:** While the ScoutDNS desktop client is a helpful addition, the lack of a mobile client is problematic for some users, making the solution a poor fit for those looking for that option.
- **Automated reporting:** Though the reporting platform is comprehensive and can provide very detailed analysis, there is currently no option for scheduling and automating report creation, which may be an issue, particularly for larger customers.
- **Threat intelligence platform integration:** The platform does not provide any predeveloped threat intelligence or its own threat intelligence platform, and though integration of such a platform can be done via API, this entails custom creation and thus increases adoption complexity.

Purchase Considerations
ScoutDNS focuses specifically on DNS security. Customers considering a single partner to enable security suite consolidation should take this into account.

The solution has very few native integrations, so those looking to integrate DNS security with mature security stacks should understand that they will most likely need to build custom API integrations, which will add to deployment time and cost.

Common use cases for adoption include MSPs looking for a DNS security partner, midsize organizations of 5,000 to 10,000 users in need of a comprehensive DNS filtering solution, education customers seeking a DNS filtering solution, and those looking for detailed reporting of DNS traffic.

Radar Chart Overview
ScoutDNS is a DNS filtering solution that continues to develop its existing features, which are enhanced by additional capabilities such as threat protection and network visibility; it's positioned in the Maturity/Platform Play quadrant. It scored well on most of our decision criteria, with lower scores in some of the more advanced categories, making it a strong Challenger.

TitanHQ: WebTitan Cloud

Solution Overview
TitanHQ is a long-established security solution provider with solutions that cover phishing, anti-spam, email protection, and DNS filtering via its SaaS WebTitan Cloud solution. WebTitan is available in three formats, WebTitan Cloud, evaluated here, as well as two specialist offerings. WebTitan Cloud for Wi-Fi is designed to protect guest hotspots, and WebTitan Cloud for Service Providers is specifically for MSPs.

The solution offers DNS filtering and other security capabilities, including content filtering, malware blocking, and phishing protection. All services can be managed via the cloud-based console or a comprehensive set of APIs. Deployment is straightforward and guided from within the management console. It requires that external IP addresses be added to WebTitan, and DNS requests are then routed to its service. The solution also provides an endpoint client that can be used to ensure DNS filtering and protection remain in place even for off-network devices. The solution can also integrate with Active Directory and Entra ID to provide insights and policy control to individual users.

The relatively simple admin console enables customers to create custom blocking rules, as well as custom messaging to inform users of DNS threats. Filtering is done using categories, and these categories are kept up to date via the solution's AI and analytics services, which rapidly identify new threats and update categories and threat databases quickly. The solution is one of the few we evaluated that offered advanced payload analysis.

Strengths
Areas where TitanHQ is particularly strong include:

- **Payload analysis:** TitanHQ is one of the few vendors to offer advanced payload analysis beyond the examination of DNS packets. The WebTitan service uses its capabilities to analyze and block malware and malicious content from download once DNS resolution has been completed.
- **Ease of adoption:** Like many of the filtering solutions evaluated, adoption is straightforward with a simple redirect of DNS requests to the new service. However, WebTitan Cloud provides additional capabilities, thanks to its endpoint client, ensuring that DNS traffic remains protected even when off-network. This addresses a potential risk and eases overall adoption by doing so.
- **SMB focus:** The threats presented by DNS impact all organizations but can be especially tricky for smaller businesses that have neither the tools nor the expertise to address the challenge. WebTitan's simple, effective, and comprehensive approach will be welcomed by its target customers.

Challenges
Areas for improvement include:

- **DNS traffic encryption:** Though WebTitan offers DNSSEC support, there is no clear description of how it handles the complex challenge presented by DNS encryption.
- **Customer focus:** Its SMB focus is likely to be off-putting for larger customers, and they will need to determine whether WebTitan offers the commercial and technical support larger organizations need.
- **Reporting:** The management console offers basic reporting, which may not meet the needs of some organizations, especially larger ones. However, basic reporting is likely to be satisfactory for WebTitan's target market.

Purchase Considerations
The solution targets SMBs and MSPs, and these are the organizations that should consider it. Larger organizations are unlikely to find the commercial support they need.

This solution is well suited to SMBs looking to enhance their DNS security, MSPs seeking a DNS security partner, and those needing to apply DNS security to Wi-Fi hotspot infrastructure, especially those providing public Wi-Fi.

Radar Chart Overview
TitanHQ offers good DNS security capabilities across its portfolio and continues to work in developing its strong technology suite; it's positioned in the Maturity/Platform Play quadrant. It scored well on the majority of our categories, with slightly lower scores in some of our specialist categories, including DNS encryption and resilience, positioning the vendor as a Challenger in our report.

WatchGuard: DNSWatch

Solution Overview
WatchGuard is a security company that offers a range of protection covering the network perimeter, endpoints, and identity. DNSWatch is its SaaS-based DNS filtering solution, which works alongside DNSWatchGO, a client agent designed to provide off-network DNS protection.

DNSWatch is a service designed to detect and block potentially dangerous DNS connections. The service can be accessed in three ways: via its built-in integration with its own WatchGuard firewalls, through DNS redirection, or via its DNSWatchGO client.

The DNSWatchGO client is available only on Windows and ChromeOS at this time. The client is lightweight and, once installed, sends all endpoint DNS requests to the DNSWatch service. DNSWatch uses threat intelligence to maintain a list of potentially malicious sites, with new threats quickly added to the central database. When potentially malicious traffic is identified, the connection is blocked and traffic is rerouted to DNSWatch servers for further investigation. Command-and-control callbacks, phishing attacks, and data exfiltration attempts are automatically blocked.

Management is done centrally, with policies created for both clients and firewalls from a single interface.

A useful addition is the solution's security awareness training. Users who click on malicious links are redirected to educational materials to highlight the warning signs of malicious content. This was not seen in other vendors evaluated.

Strengths
Areas where WatchGuard is particularly strong include:

- **DNS resilience:** The solution provides a range of resilience capabilities. Its cloud design enables resilience and scale, and using DNSWatch with its on-premises firewalls or DNS servers enables solutions to be built in HA mode.
- **Flexibility:** The service provides a good range of capabilities for installation with support for a firewall-based service, an endpoint client, and simple DNS redirection, allowing this solution to be integrated into most environments. WatchGuard also offers a number of different licensing options, as well as a strong MSP community that can offer the solution as a service.
- **User education:** DNSWatch was the only product evaluated that included user awareness training as part of its solution. This is a helpful learning tool, with users redirected to educational materials in the event they click on potentially malicious locations.

Challenges
Areas for improvement include:

- **Client support:** The DNSWatchGO client is a valuable capability to help protect off-network devices, but there's no client for macOS or mobile devices—it's available only on Windows and ChromeOS at this time.
- **Security stack integration:** As an endpoint solution, DNSWatchGO does not necessarily integrate with the wider security stack. Because it is a relatively self-contained solution, this may not be a concern, but customers who would like to ensure reporting and orchestration with other tools in their stack will need to determine if it will meet their needs.

Purchase Considerations
DNSWatch is a simple-to-use and effective product. It is aimed at the SMB market, so larger enterprises will need to evaluate whether this product, particularly from a commercial and support basis, would be suitable.

Agent support is for Windows and ChromeOS only, so customers with other environments looking for off-network support will need to consider other options.

Common use cases include SMBs looking for an effective DNS filtering solution, those needing off-network protection for a Windows or ChromeOS client base, and MSPs seeking a DNS filtering technology partner.

Radar Chart Overview
DNSWatch is a well-established DNS filtering solution, positioning WatchGuard in the Maturity/Feature Play quadrant. While the solution scored well on most of our decision criteria, it didn't score as well as some of its competitors and is a Challenger in this report.

6. Analyst's Outlook

The DNS security space falls into two basic approaches, and those evaluating solutions should consider which is most appropriate to meet their needs.

- DNS filtering vendors offer a straightforward approach. These vendors enable existing infrastructure to reroute DNS requests to a filtering service where malicious requests can be quickly identified and threats stopped, ensuring users never reach harmful content. These services are ideal for those looking for a simple solution requiring little change.
- DNS security vendors go beyond this, offering DNS filtering as part of a more comprehensive solution. These vendors may also offer capabilities such as traffic analysis, broader integration with existing tools, and more detailed payload threat analysis, and may offer adjacent technologies such as DHCP and IP address management. These solutions can often be seen bundled together as DDI platforms. However, DDI platforms are only included in this report where they offer DNS security as a discrete service that does not require use of the other components. Those requiring more comprehensive DNS security, which may include adjacent technology such as IP and DHCP management, should consider platform vendors.

The majority of vendors offer mature solutions that continue to build on established DNS security tools. Still, there is innovation in the space, with the use of threat intelligence, the adoption of DNS encryption, and, of course, the use of AI to help tackle increasingly complex challenges in an area that remains an ongoing target for cybercriminals.

Prospective customers should also consider the following in their evaluation:

- **Deployment model.** Many vendors offer their DNS security product as a SaaS solution, easy to consume and integrate with existing infrastructure. However, there are cases where an on-premises approach is appropriate; for example, in organizations that prefer to avoid using the cloud, or those that need additional capabilities, such as DNS performance acceleration. For the latter, a number of vendors offer hardware appliances that could help in both protecting and improving DNS performance. Those who wish to improve performance and resilience on existing DNS estates should consider on-premises appliances. Those who are looking for simple, non-disruptive DNS security improvement should consider SaaS vendors.
- **Off-network protection.** This is important for those who wish to ensure DNS security is maintained when devices are no longer connected to organizational infrastructure. This is usually achieved by vendors that offer an endpoint client, which will ensure all DNS traffic continues to be effectively filtered regardless of location. Those with a large number of mobile or remote workers should consider solutions that come with off-network clients.

DNS security should be a priority for every organization, but it continues to be an area that doesn't get the attention many other security topics get. Effective DNS security can greatly help to reduce risk by identifying threats earlier in the attack chain to make mitigation more effective. An investment in the right DNS security technology will provide significant value.

To learn about related topics in this space, check out the following GigaOm Radar reports:

- GigaOm Radar for DDI
- GigaOm Radar for Endpoint Detection and Response
- GigaOm Radar for Next-Generation Firewalls

7. Methodology

For more information about our research process for Key Criteria and Radar reports, please visit our Methodology.

8. About Paul Stringfellow

Paul Stringfellow has more than 25 years of experience in the IT industry helping organizations of all kinds and sizes use technology to deliver strong business outcomes. Today, that work focuses mainly on helping enterprises understand how to manage their data to ensure it is protected, secure, compliant, and available. He is still very much a "hands-on" practitioner and continues to be involved in a diverse range of data projects. Paul has been recognized across the industry and has spoken at many industry, vendor, and community events. He writes for a number of industry publications to share his enthusiasm for technology and to help others realize its value.

Paul hosts his own enterprise technology webcast and writes regularly on his blog.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright

© Knowingly, Inc. 2024 *"GigaOm Radar for Domain Name System (DNS) Security"* is a trademark of Knowingly, Inc. For permission to reproduce this report, please contact sales@gigaom.com.

GIGAOM
Knowingly Corporation
3905 State Street #7-448
Santa Barbara, CA 93105-5107

Subscribe to our monthly analyst insights newsletter

Stay on top of emerging trends by joining our newsletter, a monthly publication from our leading network of analysts.

SUBSCRIBE NOW

Research
- Methodology
- Research Calendar
- Analyst Videos
- AI, Data & Analytics
- Security & Risk
- Cloud, Infrastructure & Management
- DevOps
- Network & Edge
- People, Processes, & Applications
- View All Research

For Vendors
- Customer Centric Enablement and Activation
- Total Cost of Ownership & Engineering Benchmarks
- Radars
- Key Criteria
- Advisory Services
- Enterprise Subscription
- Value Engineering
- Vendor Marketing Content Review

Insights
- Case Studies
- Blog
- Press Room

Company
- Why GigaOm
- Our Team
- Partners
- Careers
- Contact us

Privacy Policy MSA Terms of Service Code of Conduct

© GigaOm All Rights Reserved 2024