



KEY FINDINGS FOR DNS MONITORING AND ANALYSIS

298,000
request timeouts

• Timeouts will have an impact on application performance and user experience. If associated with fee-based API driven services you may be overcharged.

35%
of request timeouts

• Sauce Labs, a cloud-based automated testing service is causing 35% of timeouts. This should be investigated to ensure you're not being billed for this traffic.

1,160
AAAA look-ups

• Thousands of IPv6 requests have been potentially causing 2 – 4 second delays for clients and applications. This should be fixed immediately.

15,000
DNS response errors

• DNS errors may be caused by misconfiguration. Fixing these may resolve application issues and slowness.

See the Appendix for DNS Monitoring dashboards

INDUSTRY FACTS

- **DNS errors and issues cause greater than 20%** of Internet and application outages – [Ars Technica](#)
- **A DNS Dashboard** for performance, availability, and risk mitigation is recommended best practice for any enterprise by DHS and the ITSRA working group along with ICANN – [U.S. Department of Homeland Security](#)

DNS MONITORING AND ANALYSIS – VALUE



Cost Savings

# of people on DNS/Network team	2	XYZ Corp
% of time spent per month troubleshooting DNS issues	20%	XYZ Corp
Average salary of DNS Admin	\$75,867	Glassdoor
Annual labor savings	\$18,208	

Risk Mitigation

Annual DNS unplanned downtime across all domains (hours)	8.75	Verisign
Potential reduction in downtime using ExtraHop	10%	TechValidate Survey
Downtime cost per hour	\$100,000	IDC
Savings due to reduction in downtime risk	\$87,500	

Total Annual Savings

\$105,708

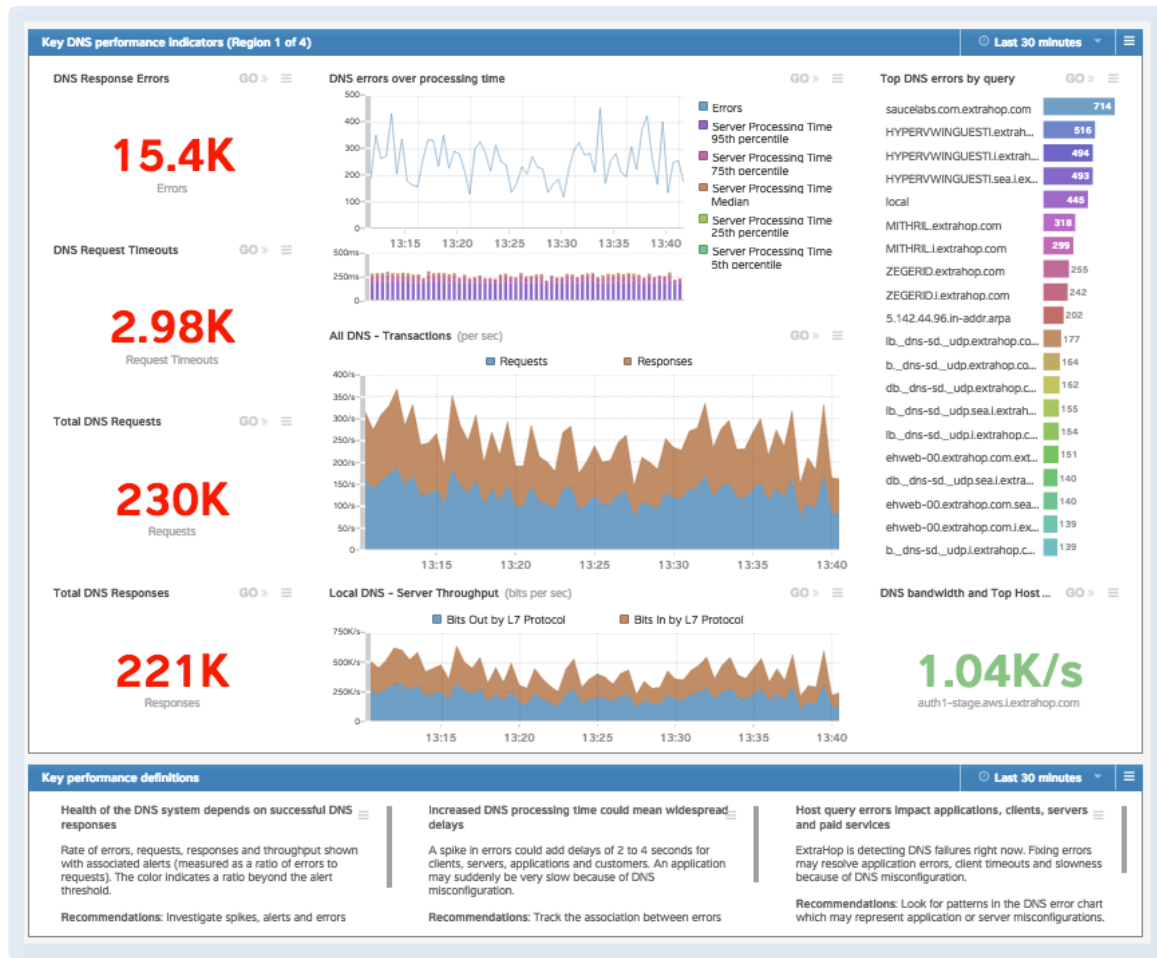
BUSINESS VALUE

- Force-multiplier for the Network, Application, and Security teams – Shorten time to remediation by up to 50%
- Prevent overcharges from fee-based API driven subscription services
- Performance improvement opportunity impacting revenue
- Increase cross-team knowledge and understanding of the importance of DNS
- If outsourcing DNS, ensure accountability and SLAs of managed service provider

DNS MONITORING AND ANALYSIS DASHBOARD



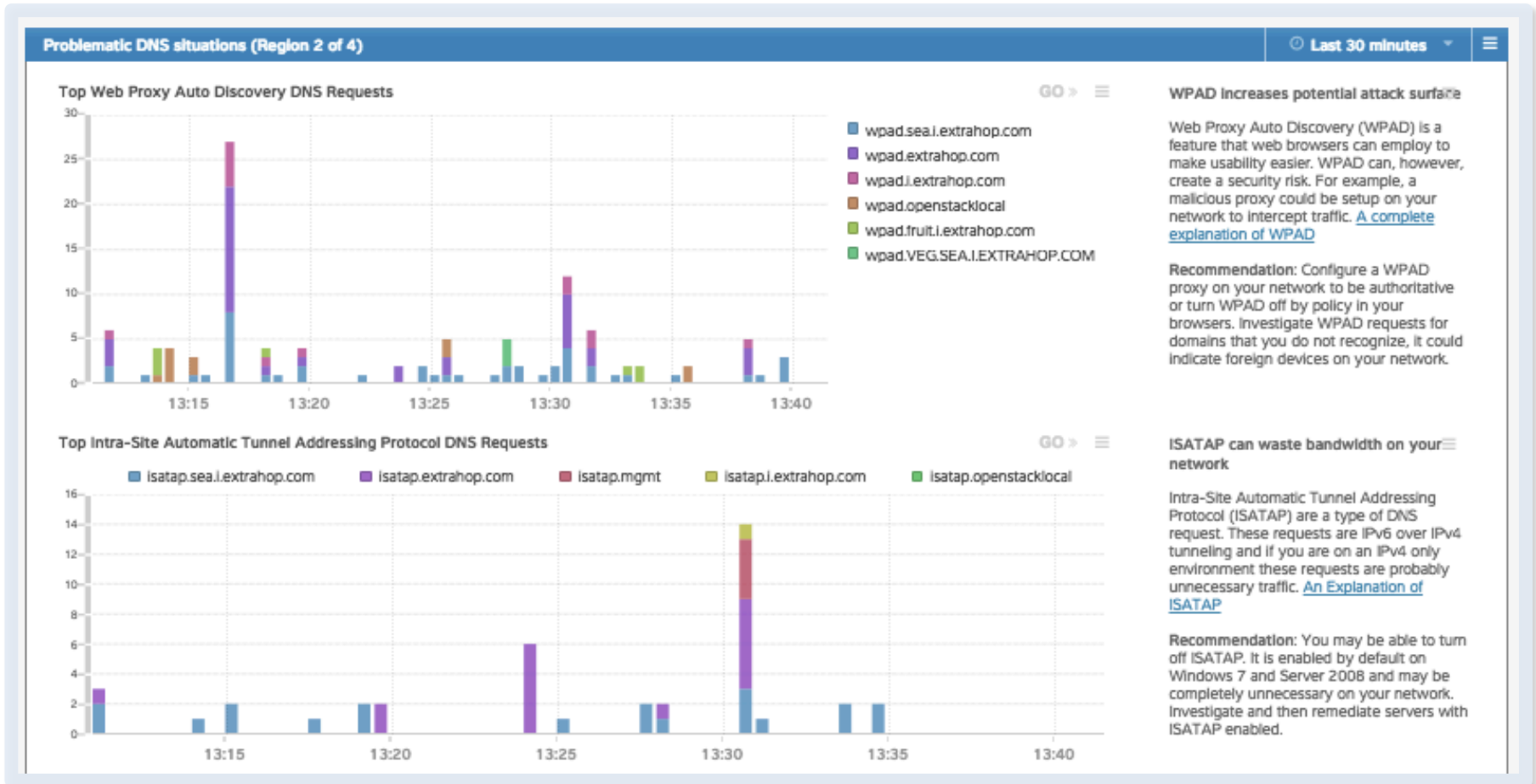
DNS errors and issues cause greater than 20% of Internet and application outages. DNS response errors and request timeouts can cause performance issues for application users. Furthermore, DNS is a common and vulnerable attack vector for botnets running distributed denial of service (DDOS) attacks. This dashboard surfaces DNS metrics that can warn you of potential performance issues or security vulnerabilities in your environment.



DNS MONITORING AND ANALYSIS



This dashboard displays instances of two types of DNS requests that can affect the performance and security of your network. The first is WPAD, which can provide an attack vector into your network, and the second is ISATAP, which wastes bandwidth if enabled unnecessarily.

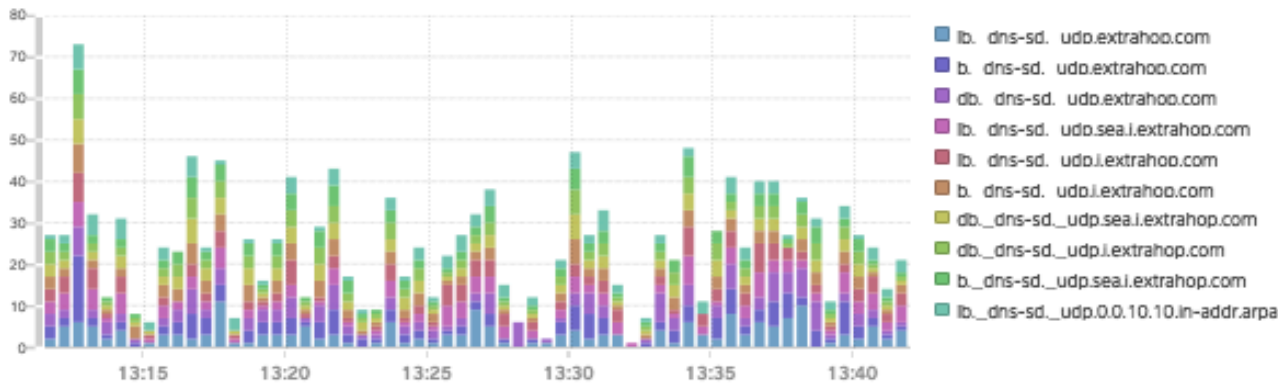


DNS MONITORING AND ANALYSIS



This area of the DNS Monitoring dashboard shows two types of DNS queries or lookups that are often enabled on networks even when unnecessary. Both DNS-SD and IPV6 lookups can cause latency and timeouts if they're enabled on your network and they shouldn't be. Fixing this improves user experience.

Top Multicast (DNS-SD) Queries (per 30s)

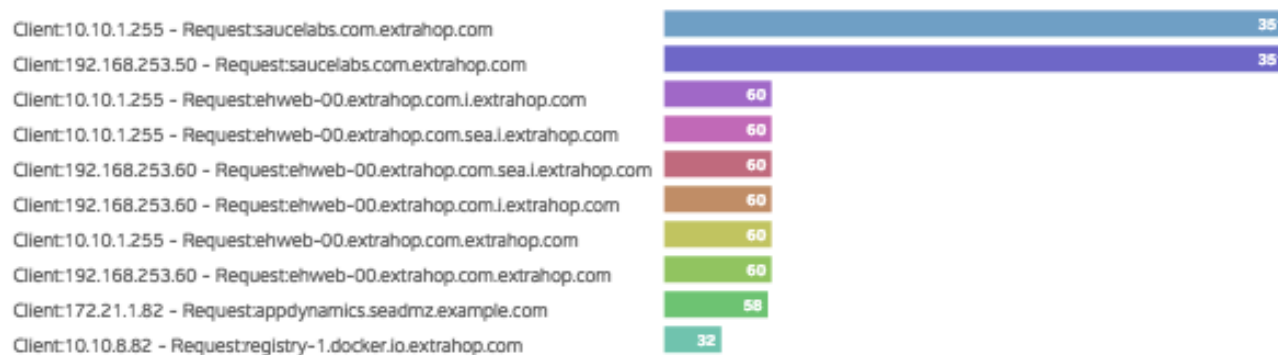


DNS-SD can waste bandwidth and make troubleshooting difficult

DNS-SD is not regular DNS but related to multicast DNS (sometimes called Bonjour in Apple environments). [Multicast DNS Information in detail](#)

Recommendation: Multicast DNS may be unnecessary on your network. Find and disable MDNS traffic sources.

DNS IPV6 After Error



Delays will result from IPV6 lookups in an IPV4 environment

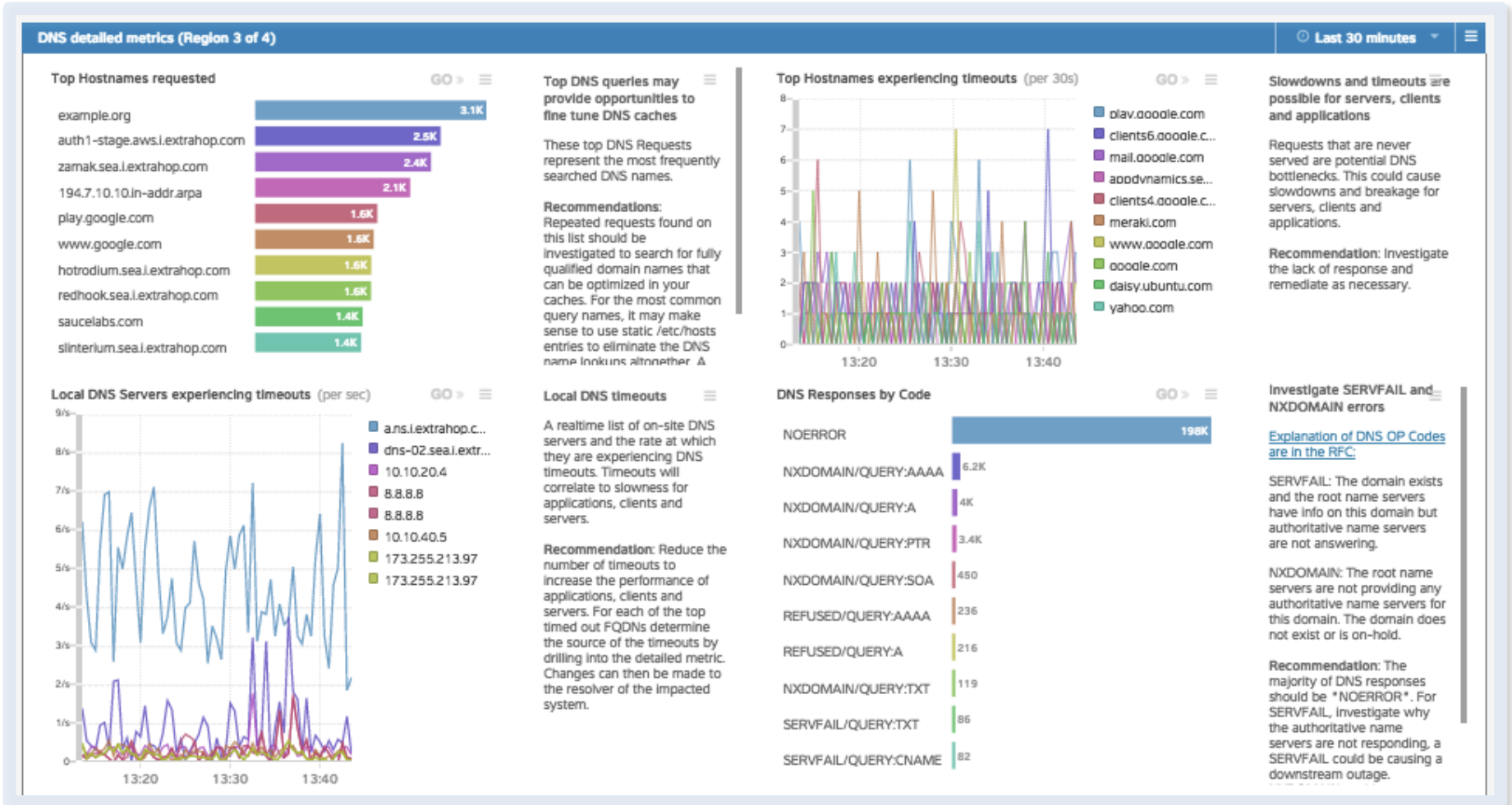
AAAA detection on IPV4 network will show desktop and server operating systems increasingly that are IPV6 enabled but are primarily using IPV4. OSes may use IPV6 DNS lookups even when it is completely unnecessary. Delays and issues may result from AAAA lookups in IPV4 networks as the applications wait for both IPV4 and IPV6 results to return, creating a block.

Recommendation: Configure your DNS to server the proper NXDOMAIN requests to avoid a lag of 2-4s as the client waits for a timeout.

DNS MONITORING AND ANALYSIS



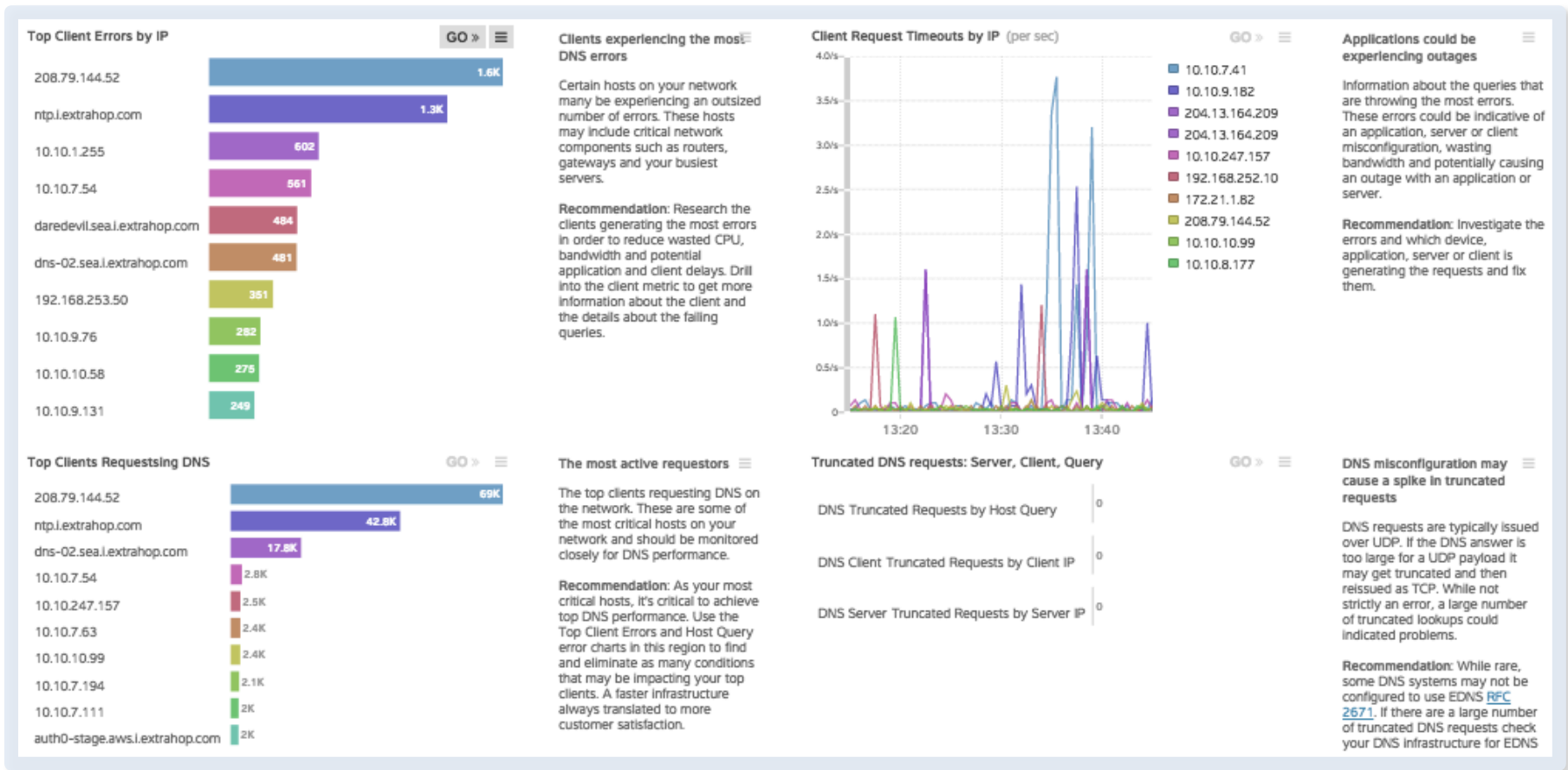
This section of the DNS Monitoring dashboard shows local DNS servers and Hostnames experiencing timeouts, both of which negatively impact application performance. The dashboard also shows opportunities for optimizing your most accessed hostnames, and tracking error codes to assure everything is running smoothly.



DNS MONITORING AND ANALYSIS



This area of the dashboard is all about clients. You can see which clients are the most active requesters, which are experiencing errors, and which are getting timeouts. Trends shown in this section can help you improve DNS performance for the most active clients on your network.



DNS MONITORING AND ANALYSIS



DNS lookup and testing tools are another useful way to investigate DNS performance and corroborate the insights you're getting from ExtraHop. The dashboard includes links to some external testing services so you can learn as much as possible about your DNS environment.

The screenshot displays a dashboard interface with a blue header bar. The header contains the text "Validate (Region 4 or 4)" on the left and "Last 30 minutes" with a dropdown arrow on the right. The main content area is divided into three columns. The left column features two logos: ARIN (American Registry for Internet Numbers) and RIPE NCC (RIPE NETWORK COORDINATION CENTRE). The middle column has two sections: "ARIN WHOIS LOOKUP" with a brief description of the service and a link to "RIPE DNS Check" with its description. The right column contains "ARIN on-line whois lookup" with a search input field and a "SEARCH Whois" button, and "RIPE on-line DNSCheck service" with a "Domain name:" input field.