ExtraHop

ExtraHop for IT Performance

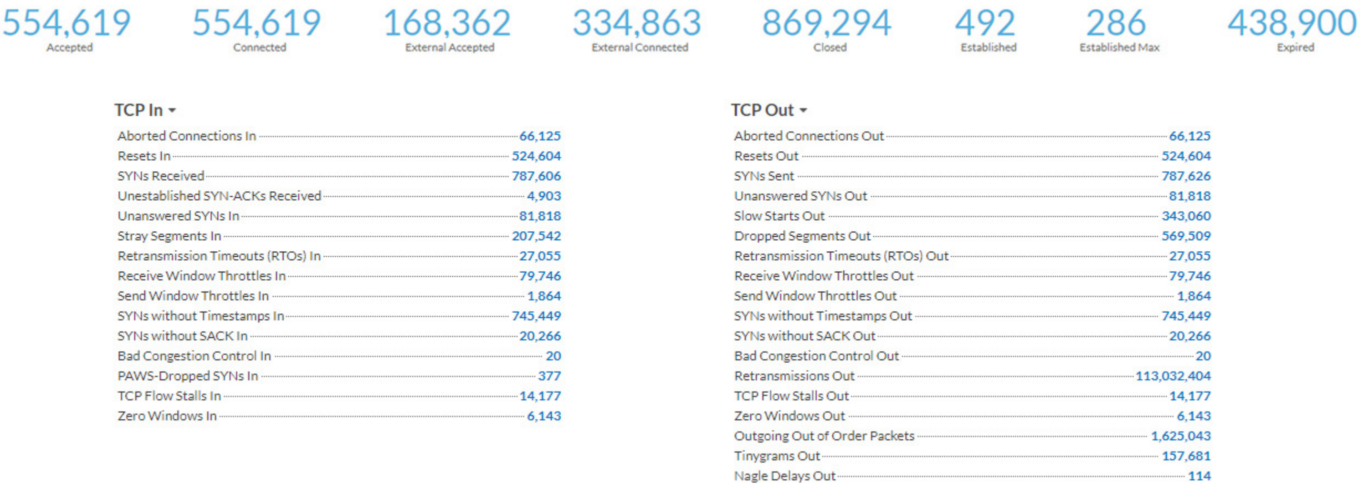
Introduction

ExtraHop is a network traffic analysis platform that has been an industry leading NPM solution for over 15 years. ExtraHop focuses on extracting the most important details from network traffic before storing the packet, making it faster and easier for IT, network, and application teams to solve complex problems in minutes rather than hours.

But ExtraHop is not only an NPM tool. ExtraHop uses the same network data to find security risks, identify compliance issues, and detect threats in real time. Integrations with knowledge bases like MITRE ATT&CK and other powerful security tools like Crowdstrike and Splunk enable automated triage and response.

When IT and security pros work together, magic happens. Sharing a unified platform fosters collaboration which breaks down divisions and creates a shared understanding of network operations and security responsibilities.

Deep TCP Analysis in just a few clicks...



554,619	554,619	168,362	334,863	869,294	492	286	438,900
Accepted	Connected	External Accepted	External Connected	Closed	Established	Established Max	Expired

TCP In ▾	
Aborted Connections In	66,125
Resets In	524,604
SYNs Received	787,606
Unestablished SYN-ACKs Received	4,903
Unanswered SYNs In	81,818
Stray Segments In	207,542
Retransmission Timeouts (RTOs) In	27,055
Receive Window Throttles In	79,746
Send Window Throttles In	1,864
SYNs without Timestamps In	745,449
SYNs without SACK In	20,266
Bad Congestion Control In	20
PAWS-Dropped SYNs In	377
TCP Flow Stalls In	14,177
Zero Windows In	6,143

TCP Out ▾	
Aborted Connections Out	66,125
Resets Out	524,604
SYNs Sent	787,626
Unanswered SYNs Out	81,818
Slow Starts Out	343,060
Dropped Segments Out	569,509
Retransmission Timeouts (RTOs) Out	27,055
Receive Window Throttles Out	79,746
Send Window Throttles Out	1,864
SYNs without Timestamps Out	745,449
SYNs without SACK Out	20,266
Bad Congestion Control Out	20
Retransmissions Out	113,032,404
TCP Flow Stalls Out	14,177
Zero Windows Out	6,143
Outgoing Out of Order Packets	1,625,043
Tinygrams Out	157,681
Nagle Delays Out	114

Figure 1. A sample of the metrics available in the ExtraHop platform for drilling into TCP performance

Common TCP problems, such as retransmissions, timeouts, window errors, resets, and others, can be quickly identified and addressed using ExtraHop's solution. This streamlines the process of troubleshooting network issues by pulling what matters to the front, helping network pros find the details they need without spending hours crawling through packet captures.

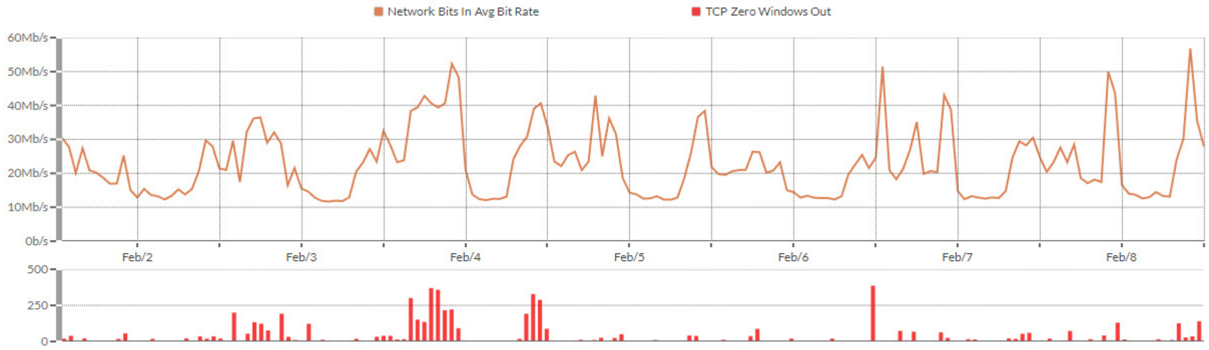


Figure 2. All metrics can be combined into charts and graphs for comparison, overlay, and analysis. These charts can be saved as dashboards for reports or on-demand viewing

ExtraHop enables the visualization and comparison of thousands of metrics, providing the insights necessary for solving complex network problems. The breadth of data available helps analysts scan dozens of KPIs quickly and accelerates the mean time to resolution. This broad brush first pass is often more valuable than depth alone when every minute counts.

With the ability to quickly review key performance indicators from the link layer to the application data, without the need for extensive analysis of PCAPs or reliance on bestguess scenarios, network professionals can rapidly determine the root cause of issues and return to normal operations.

Industry leading decryption capability and scale

100Gbs decrypted and analyzed in real-time with a single appliance.

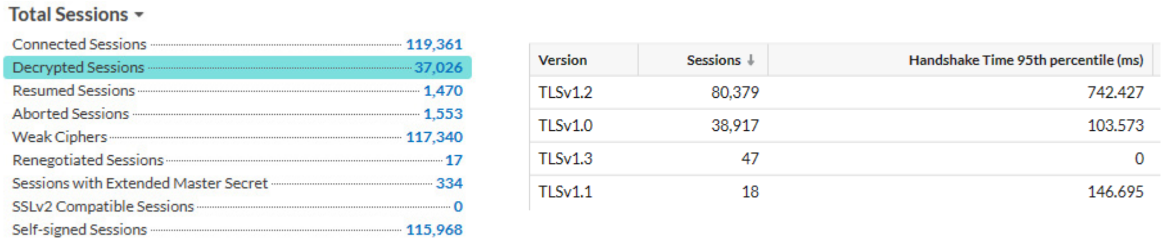
ExtraHop is the only datacenter scalable NDR solution on the market, there is no competition. This comes from our 15 years of experience building an NPM platform to provide better features and functionality than legacy solutions like Riverbed and Netscout. To compete you need to scale. We do, and we do it better.

What about decryption?

ExtraHop performs decryption out-of-band, ensuring that security is never compromised and applications are not impacted. The solution is capable of performing line rate decryption, up to its full analysis capacity, without sacrificing performance.

Decryption of legacy public key encryption is mostly table stakes these days. The reality is that in the modern era this type of encryption has fallen off in favor of quantum resistant perfect forward secrecy standards like TLS 1.3 where ephemeral session keys are used instead.

ExtraHop is the only solution on the market able to decrypt TLS 1.3 network traffic.



Total Sessions ▾

Connected Sessions	119,361
Decrypted Sessions	37,026
Resumed Sessions	1,470
Aborted Sessions	1,553
Weak Ciphers	117,340
Renegotiated Sessions	17
Sessions with Extended Master Secret	334
SSLv2 Compatible Sessions	0
Self-signed Sessions	115,968

Version	Sessions ↓	Handshake Time 95th percentile (ms)
TLSv1.2	80,379	742.427
TLSv1.0	38,917	103.573
TLSv1.3	47	0
TLSv1.1	18	146.695

Figure 3. TLS session and certificate information is broken down across all network transactions. Details about versions, SNIs, cipher suites, and much more are available.

Application layer analysis *without* performance loss

ExtraHop provides comprehensive analysis of over 70 Layer 7 protocols, including web services, authentication, administration, databases, terminals, file services, and storage, among others. With its powerful decoding capabilities, ExtraHop delivers detailed insights into application troubleshooting and performance analysis in a matter of seconds or minutes, not hours or days. By providing a comprehensive and in-depth understanding of network traffic, ExtraHop helps organizations ensure optimal performance and security of their applications.

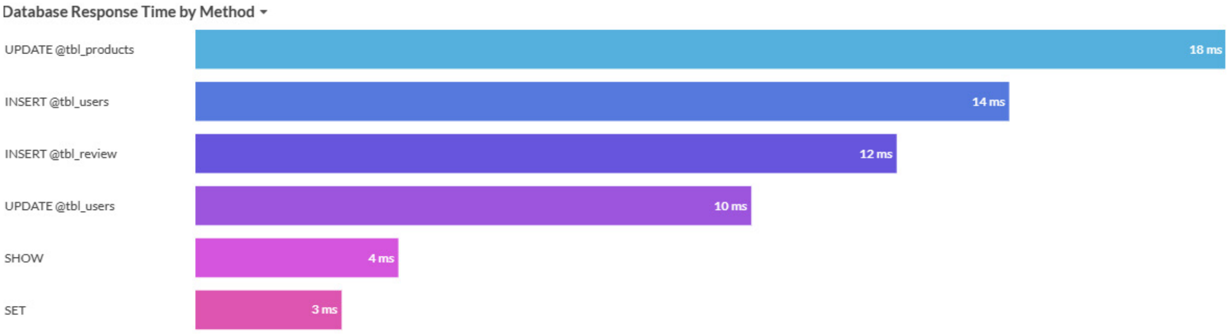
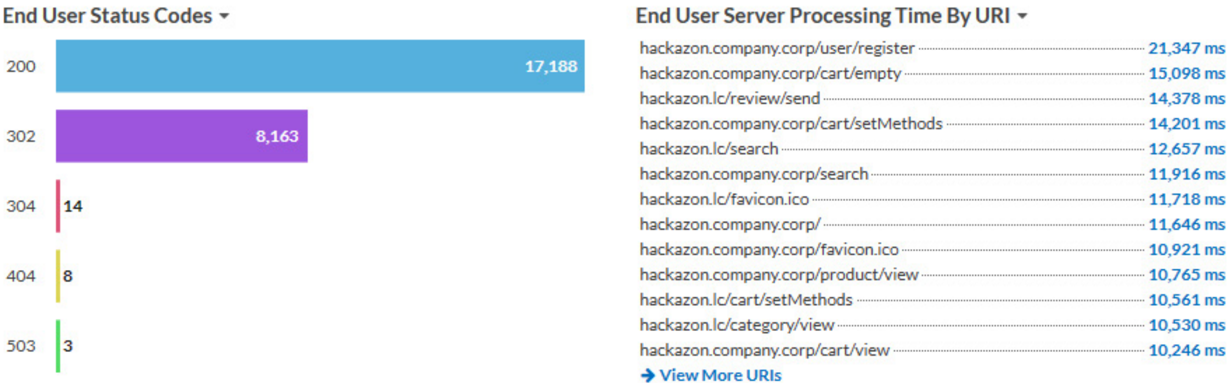
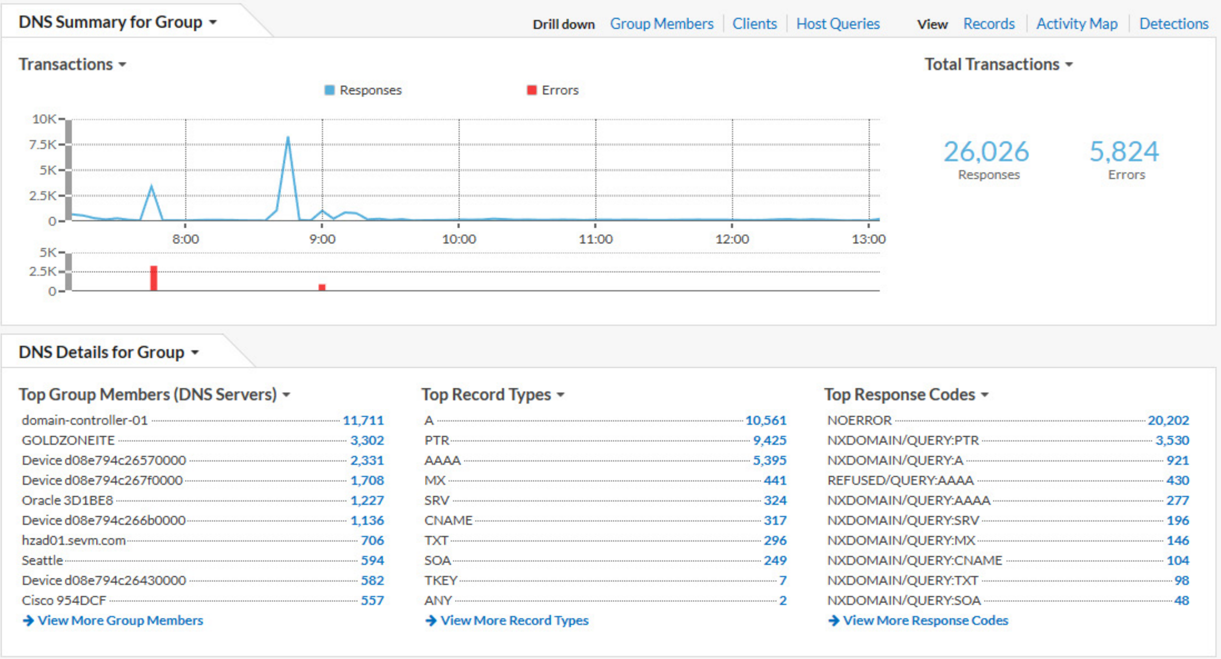


Figure 4. Finding a slow database transaction in a sea of servers, tables, and clients doesn't require logs or agents; it can be done instantly and passively from packets



hackazon.company.corp/user/register	21,347 ms
hackazon.company.corp/cart/empty	15,098 ms
hackazon.lc/review/send	14,378 ms
hackazon.company.corp/cart/setMethods	14,201 ms
hackazon.lc/search	12,657 ms
hackazon.company.corp/search	11,916 ms
hackazon.lc/favicon.ico	11,718 ms
hackazon.company.corp/	11,646 ms
hackazon.company.corp/favicon.ico	10,921 ms
hackazon.company.corp/product/view	10,765 ms
hackazon.lc/cart/setMethods	10,561 ms
hackazon.lc/category/view	10,530 ms
hackazon.company.corp/cart/view	10,246 ms

Figure 5. Web server errors, slowness, and unexpected behavior can be broken down to the URI level for rapid remediation



Total Transactions	
26,026	5,824
Responses	Errors

Top Group Members (DNS Servers) ▾

domain-controller-01	11,711
GOLDZONEITE	3,302
Device d08e794c26570000	2,331
Device d08e794c267f0000	1,708
Oracle 3D1BE8	1,227
Device d08e794c266b0000	1,136
hzad01.sevm.com	706
Seattle	594
Device d08e794c26430000	582
Cisco 954DCF	557

→ View More Group Members

Top Record Types ▾

A	10,561
PTR	9,425
AAAA	5,395
MX	441
SRV	324
CNAME	317
TXT	296
SOA	249
TKEY	7
ANY	2

→ View More Record Types

Top Response Codes ▾

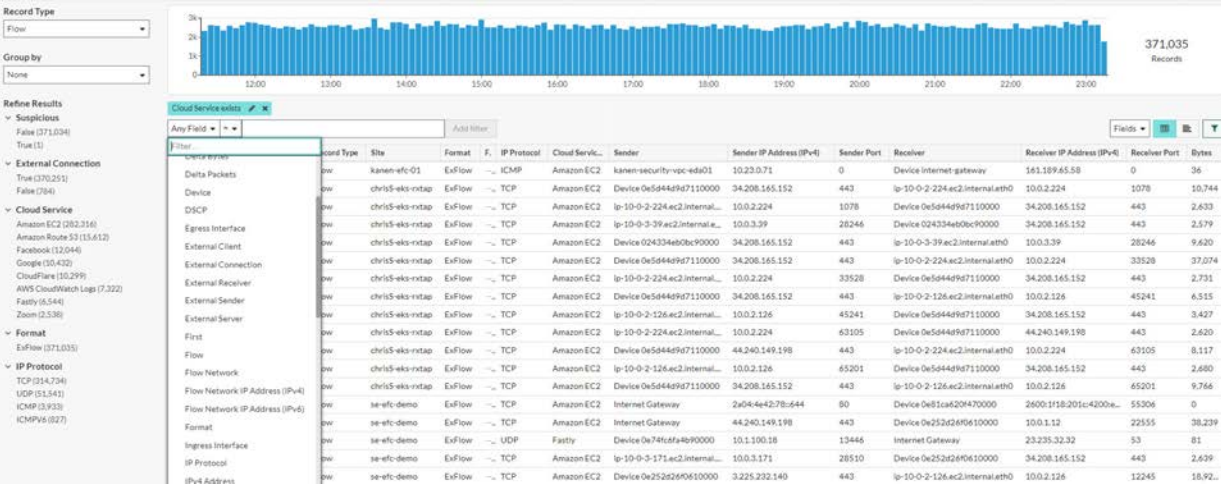
NOERROR	20,202
NXDOMAIN/QUERY:PTR	3,530
NXDOMAIN/QUERY:A	921
REFUSED/QUERY:AAAA	430
NXDOMAIN/QUERY:AAAA	277
NXDOMAIN/QUERY:SRV	196
NXDOMAIN/QUERY:MX	146
NXDOMAIN/QUERY:CNAME	104
NXDOMAIN/QUERY:TXT	98
NXDOMAIN/QUERY:SOA	48

→ View More Response Codes

Figure 6. Other protocols like DNS, DHCP, and auth mechanisms are immensely important - ExtraHop can break all of these down and instantly spot spikes in errors for name resolutions, leases, and auth failures

Transactional records for every flow

ExtraHop metrics deliver quick access to errors, latency, transaction counts, and more. When you need to go deeper Records give you in-depth information on each flow and exchange, which can be easily accessed by drilling down from metrics or using our visual query language.



Record Type: Flow

Group by: None

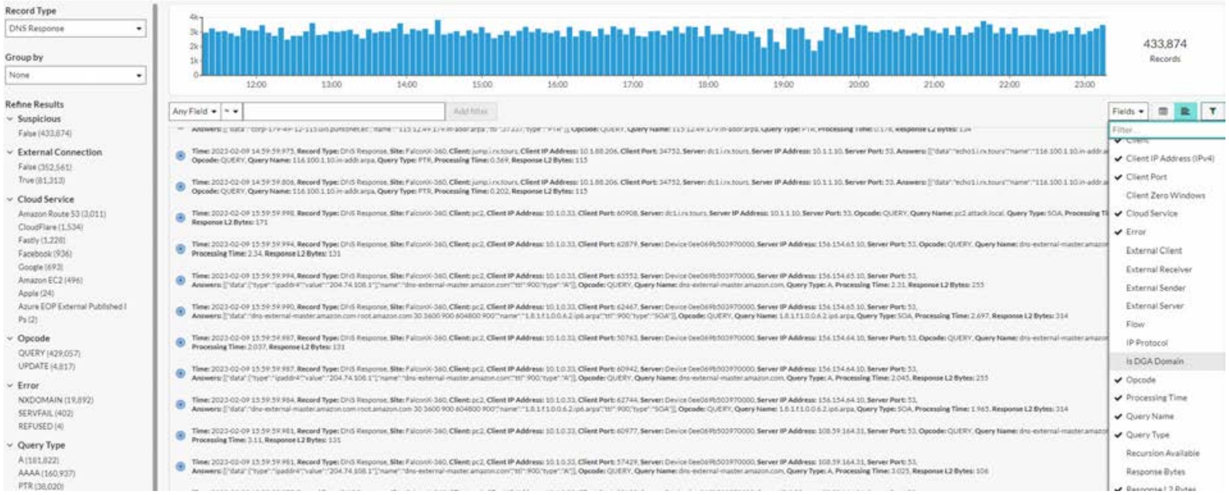
371,035
Records

Cloud Service exists

Refine Results
- Suspicious
  - False (371,034)
  - True (1)
- External Connection
  - True (370,251)
  - False (784)
- Cloud Service
  - Amazon EC2 (282,316)
  - Amazon Route 53 (15,612)
  - Facebook (12,044)
  - Google (10,432)
  - CloudFlare (10,299)
  - AWS CloudWatch Logs (7,322)
  - Fastly (6,544)
  - Zoom (2,538)
- Format
  - ExFlow (371,035)
- IP Protocol
  - TCP (314,734)
  - UDP (51,541)
  - ICMP (3,933)
  - ICMPV6 (827)

cord Type	Site	Format	F.	IP Protocol	Cloud Servic...	Sender	Sender IP Address (IPv4)	Sender Port	Receiver	Receiver IP Address (IPv4)	Receiver Port	Bytes
ow	kanen-efc-01	ExFlow	-..	ICMP	Amazon EC2	kanen-security-vpc-eda01	10.23.0.71	0	Device internet-gateway	161.189.65.58	0	36
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 0e5d44d9d7110000	34.208.165.152	443	ip-10-0-2-224.ec2.internal.eth0	10.0.2.224	1078	10,744
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-2-224.ec2.internal...	10.0.2.224	1078	Device 0e5d44d9d7110000	34.208.165.152	443	2,633
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-3-39.ec2.internal.e...	10.0.3.39	28246	Device 024334eb0bc90000	34.208.165.152	443	2,579
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 024334eb0bc90000	34.208.165.152	443	ip-10-0-3-39.ec2.internal.eth0	10.0.3.39	28246	9,620
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 0e5d44d9d7110000	34.208.165.152	443	ip-10-0-2-224.ec2.internal.eth0	10.0.2.224	33528	37,074
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-2-224.ec2.internal...	10.0.2.224	33528	Device 0e5d44d9d7110000	34.208.165.152	443	2,731
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 0e5d44d9d7110000	34.208.165.152	443	ip-10-0-2-126.ec2.internal.eth0	10.0.2.126	45241	6,515
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-2-126.ec2.internal...	10.0.2.126	45241	Device 0e5d44d9d7110000	34.208.165.152	443	3,427
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-2-224.ec2.internal...	10.0.2.224	63105	Device 0e5d44d9d7110000	44.240.149.198	443	2,620
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 0e5d44d9d7110000	44.240.149.198	443	ip-10-0-2-224.ec2.internal.eth0	10.0.2.224	63105	8,117
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	ip-10-0-2-126.ec2.internal...	10.0.2.126	65201	Device 0e5d44d9d7110000	34.208.165.152	443	2,680
ow	chris5-eks-rxtap	ExFlow	-..	TCP	Amazon EC2	Device 0e5d44d9d7110000	34.208.165.152	443	ip-10-0-2-126.ec2.internal.eth0	10.0.2.126	65201	9,766
ow	se-efc-demo	ExFlow	-..	TCP	Amazon EC2	Internet Gateway	2a04:4e42:78::644	80	Device 0e81ca620f470000	2600:1f18:201c:4200:e...	55306	0
ow	se-efc-demo	ExFlow	-..	TCP	Amazon EC2	Internet Gateway	44.240.149.198	443	Device 0e252d26f0610000	10.0.1.12	22555	38,239
ow	se-efc-demo	ExFlow	-..	UDP	Fastly	Device 0e74fc6fa4b90000	10.1.100.18	13446	Internet Gateway	23.235.32.32	53	81
ow	se-efc-demo	ExFlow	-..	TCP	Amazon EC2	ip-10-0-3-171.ec2.internal...	10.0.3.171	28510	Device 0e252d26f0610000	34.208.165.152	443	2,639
ow	se-efc-demo	ExFlow	-..	TCP	Amazon EC2	Device 0e252d26f0610000	3.225.232.140	443	ip-10-0-2-126.ec2.internal.eth0	10.0.2.126	12245	18,92...

Figure 7. An example of a collection of flow records in the ExtraHop solution which can be filtered and searched using our powerful visual query language.



```
Answers: [{"data":"corp-179-49-12-115.on.pureone.net","name":"115.12.49.179.in-addr.arpa","ttl":37337,"type":"PTR"}], Opcode: QUERY, Query Name: 115.12.49.179.in-addr.arpa, Query Type: PTR, Processing Time: 0.178, Response L2 Bytes: 134

Time: 2023-02-09 14:59:59.973, Record Type: DNS Response, Site: FalconX-360, Client: jump.i.rx.tours, Client IP Address: 10.1.88.206, Client Port: 34732, Server: dc1.i.rx.tours, Server IP Address: 10.1.1.10, Server Port: 53, Answers: [{"data":"echo1.i.rx.tours","name":"116.100.1.10.in-addr.a
Opcode: QUERY, Query Name: 116.100.1.10.in-addr.arpa, Query Type: PTR, Processing Time: 0.369, Response L2 Bytes: 115

Time: 2023-02-09 14:59:59.806, Record Type: DNS Response, Site: FalconX-360, Client: jump.i.rx.tours, Client IP Address: 10.1.88.206, Client Port: 34732, Server: dc1.i.rx.tours, Server IP Address: 10.1.1.10, Server Port: 53, Answers: [{"data":"echo1.i.rx.tours","name":"116.100.1.10.in-addr.a
Opcode: QUERY, Query Name: 116.100.1.10.in-addr.arpa, Query Type: PTR, Processing Time: 0.202, Response L2 Bytes: 115

Time: 2023-02-09 15:59:59.998, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 60908, Server: dc1.i.rx.tours, Server IP Address: 10.1.1.10, Server Port: 53, Opcode: QUERY, Query Name: pc2.attack.local, Query Type: SOA, Processing Ti
Response L2 Bytes: 171

Time: 2023-02-09 15:59:59.994, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 62879, Server: Device 0ee069b503970000, Server IP Address: 156.154.65.10, Server Port: 53, Opcode: QUERY, Query Name: dns-external-master.amazo
Processing Time: 2.34, Response L2 Bytes: 131

Time: 2023-02-09 15:59:59.994, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 63552, Server: Device 0ee069b503970000, Server IP Address: 156.154.65.10, Server Port: 53,
Answers: [{"data":{"type":"ipaddr4","value":"204.74.108.1"},"name":"dns-external-master.amazon.com","ttl":900,"type":"A"}], Opcode: QUERY, Query Name: dns-external-master.amazon.com, Query Type: A, Processing Time: 2.31, Response L2 Bytes: 255

Time: 2023-02-09 15:59:59.990, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 62467, Server: Device 0ee069b503970000, Server IP Address: 156.154.65.10, Server Port: 53,
Answers: [{"data":"dns-external-master.amazon.com root.amazon.com 30 3600 900 604800 900","name":"1.8.1.f.1.0.0.6.2.ip6.arpa","ttl":900,"type":"SOA"}], Opcode: QUERY, Query Name: 1.8.1.f.1.0.0.6.2.ip6.arpa, Query Type: SOA, Processing Time: 2.697, Response L2 Bytes: 314

Time: 2023-02-09 15:59:59.987, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 50763, Server: Device 0ee069b503970000, Server IP Address: 156.154.64.10, Server Port: 53, Opcode: QUERY, Query Name: dns-external-master.amazo
Processing Time: 2.037, Response L2 Bytes: 131

Time: 2023-02-09 15:59:59.987, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 60942, Server: Device 0ee069b503970000, Server IP Address: 156.154.64.10, Server Port: 53,
Answers: [{"data":{"type":"ipaddr4","value":"204.74.108.1"},"name":"dns-external-master.amazon.com","ttl":900,"type":"A"}], Opcode: QUERY, Query Name: dns-external-master.amazon.com, Query Type: A, Processing Time: 2.045, Response L2 Bytes: 255

Time: 2023-02-09 15:59:59.984, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 62744, Server: Device 0ee069b503970000, Server IP Address: 156.154.64.10, Server Port: 53,
Answers: [{"data":"dns-external-master.amazon.com root.amazon.com 30 3600 900 604800 900","name":"1.8.1.f.1.0.0.6.2.ip6.arpa","ttl":900,"type":"SOA"}], Opcode: QUERY, Query Name: 1.8.1.f.1.0.0.6.2.ip6.arpa, Query Type: SOA, Processing Time: 1.965, Response L2 Bytes: 314

Time: 2023-02-09 15:59:59.981, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 60977, Server: Device 0ee069b503970000, Server IP Address: 108.59.164.31, Server Port: 53, Opcode: QUERY, Query Name: dns-external-master.amazo
Processing Time: 3.11, Response L2 Bytes: 131

Time: 2023-02-09 15:59:59.981, Record Type: DNS Response, Site: FalconX-360, Client: pc2, Client IP Address: 10.1.0.33, Client Port: 57429, Server: Device 0ee069b503970000, Server IP Address: 108.59.164.31, Server Port: 53,
Answers: [{"data":{"type":"ipaddr4","value":"204.74.108.1"},"name":"dns-external-master.amazon.com","ttl":900,"type":"A"}], Opcode: QUERY, Query Name: dns-external-master.amazon.com, Query Type: A, Processing Time: 3.025, Response L2 Bytes: 106
```

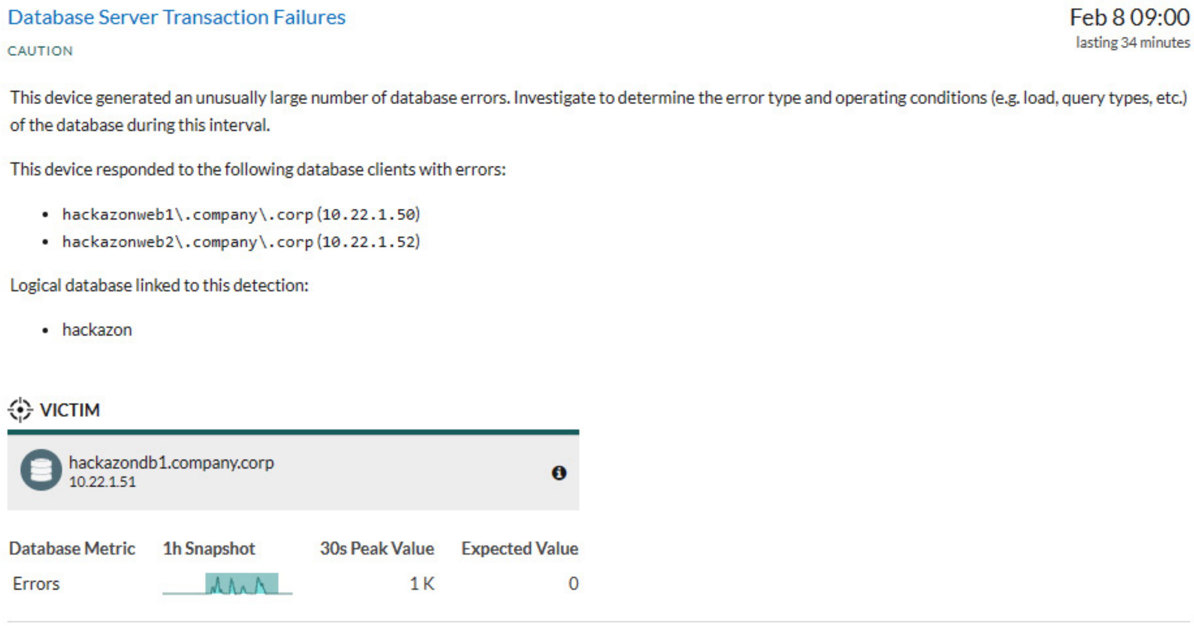
Figure 8. Records can show more detailed L7 protocols. Here is a sample of DNS transaction records.

Cloud Scale machine learning applied to over 5,000 metrics

ExtraHop harnesses the power of machine learning to provide a sophisticated and scalable network analysis solution. Our AI algorithms are run in the cloud, allowing us to process millions of models against a vast array of metrics for deep learning, neural networks, clustering, regression, and more. This enables us to quickly identify device roles, establish what is normal network behavior, and issue alerts for any anomalies. Our solution continuously evolves as it learns from changes in the network environment and insights gained are shared across all ExtraHop deployments. Additionally, our ML approach prioritizes privacy and security by tokenizing and obfuscating all metrics before they leave the customer's data center ensuring confidentiality while enabling collaboration.

What can AI do for performance monitoring?

ExtraHop AI delivers real-time, objective insight that enables users to deliver everything from increased website uptime to more efficient assembly lines to better patient care. Benefits include delivering intelligent insight for IT, enabling a proactive, data-driven approach to supporting and securing the digital experience, and helping IT teams take a proactive approach to operations. Our AI also learns from feedback to reduce the number of false positives and keep IT teams focused on the most critical issues.



Database Server Transaction Failures

CAUTION

Feb 8 09:00
lasting 34 minutes

This device generated an unusually large number of database errors. Investigate to determine the error type and operating conditions (e.g. load, query types, etc.) of the database during this interval.

This device responded to the following database clients with errors:

- `hackazonweb1\.company\.corp` (10.22.1.50)
- `hackazonweb2\.company\.corp` (10.22.1.52)

Logical database linked to this detection:

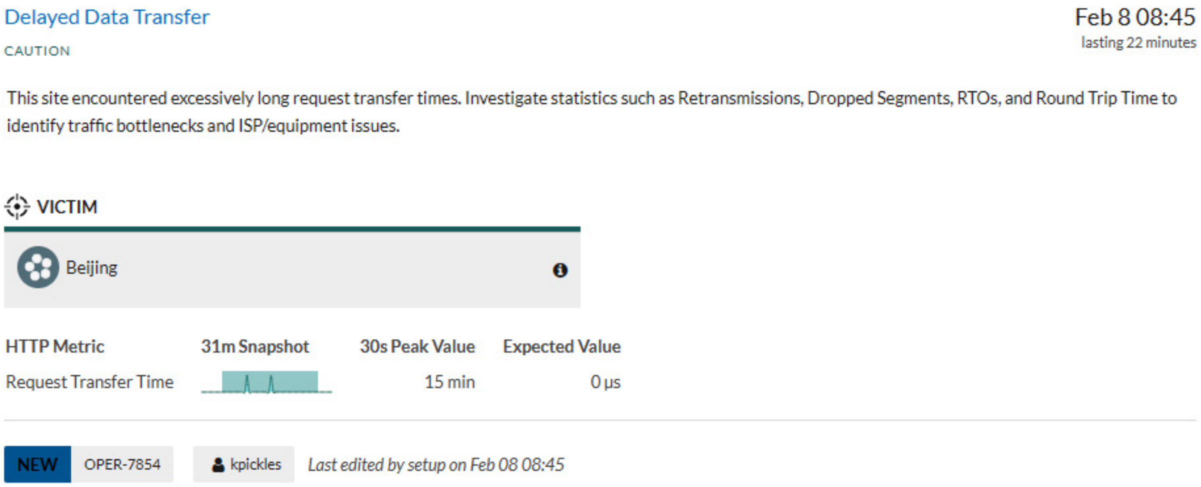
- hackazon

VICTIM

hackazondb1.company.corp
10.22.1.51

Database Metric	1h Snapshot	30s Peak Value	Expected Value
Errors		1 K	0

Figure 9. Application level error rates, latency, or anomalies are analyzed and alerts generated often before the performance impact is reported.



Delayed Data Transfer

CAUTION

Feb 8 08:45
lasting 22 minutes

This site encountered excessively long request transfer times. Investigate statistics such as Retransmissions, Dropped Segments, RTOs, and Round Trip Time to identify traffic bottlenecks and ISP/equipment issues.

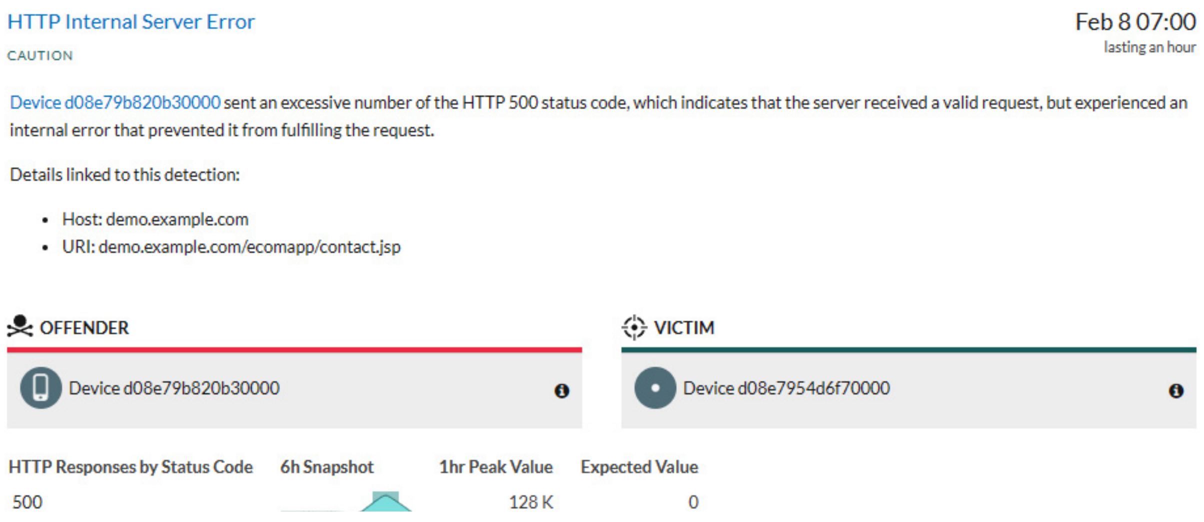
VICTIM

Beijing

HTTP Metric	31m Snapshot	30s Peak Value	Expected Value
Request Transfer Time		15 min	0 µs

Last edited by setup on Feb 08 08:45

Figure 10. Traffic to remote sites is also modeled, detection of top-talkers, site slowness, and even application layer issues that may be linked to network issues



HTTP Internal Server Error

CAUTION

Feb 8 07:00
lasting an hour

Device d08e79b820b30000 sent an excessive number of the HTTP 500 status code, which indicates that the server received a valid request, but experienced an internal error that prevented it from fulfilling the request.

Details linked to this detection:

- Host: demo.example.com
- URI: demo.example.com/ecomapp/contact.jsp

OFFENDER: Device d08e79b820b30000

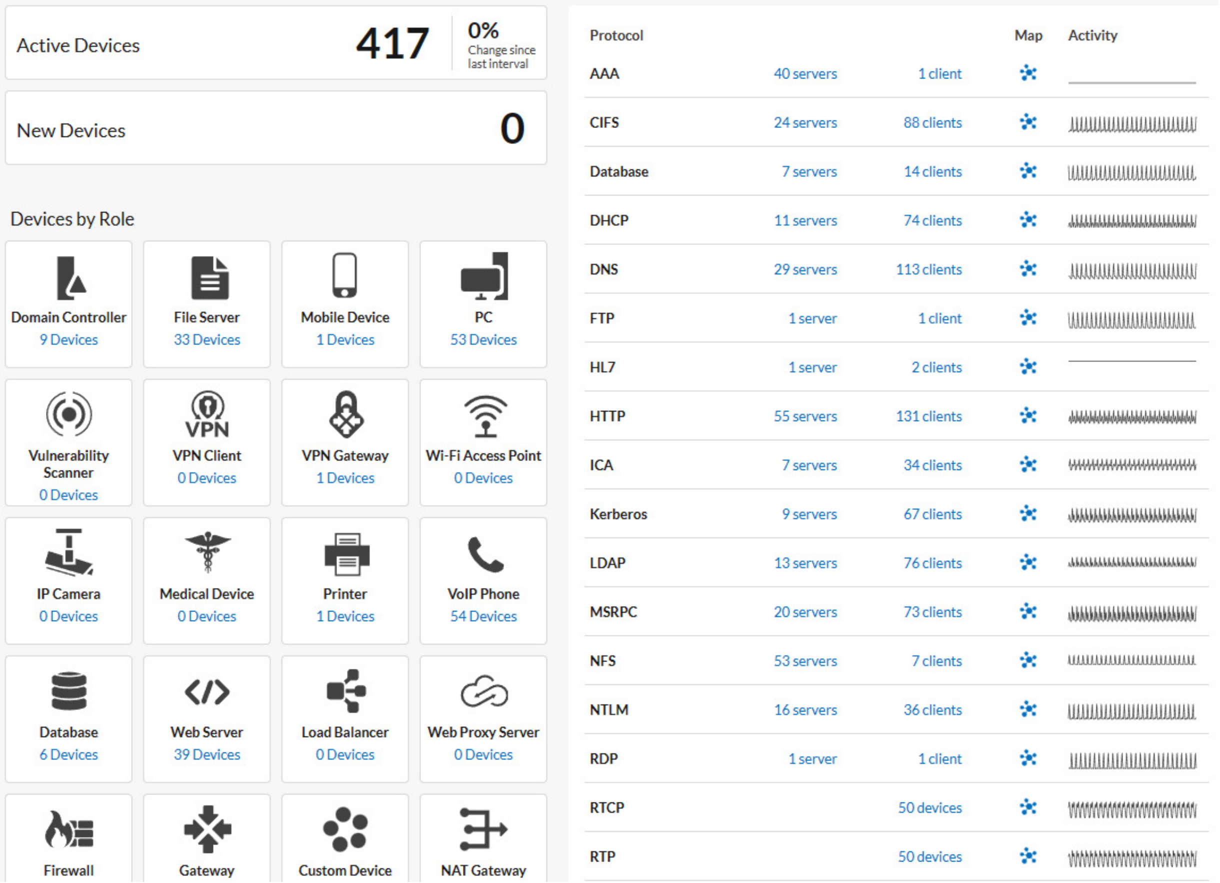
VICTIM: Device d08e7954d6f70000

HTTP Responses by Status Code	6h Snapshot	1hr Peak Value	Expected Value
500		128 K	0

Figure 11. Web servers, applications, file delivery and other communications occur over web protocols like HTTPS.

Passive asset discovery and classification

ExtraHop's solution provides real-time device classification and profiling for your network. As soon as a new device begins communication, ExtraHop begins building its profile, determining whether it is a client or a server, critical infrastructure, mobile device, or a rogue DHCP server, among others. The process of discovery, profiling, and classification happens quickly and efficiently, without the need for logs or agents.



Active Devices 417 0% Change since last interval

New Devices 0

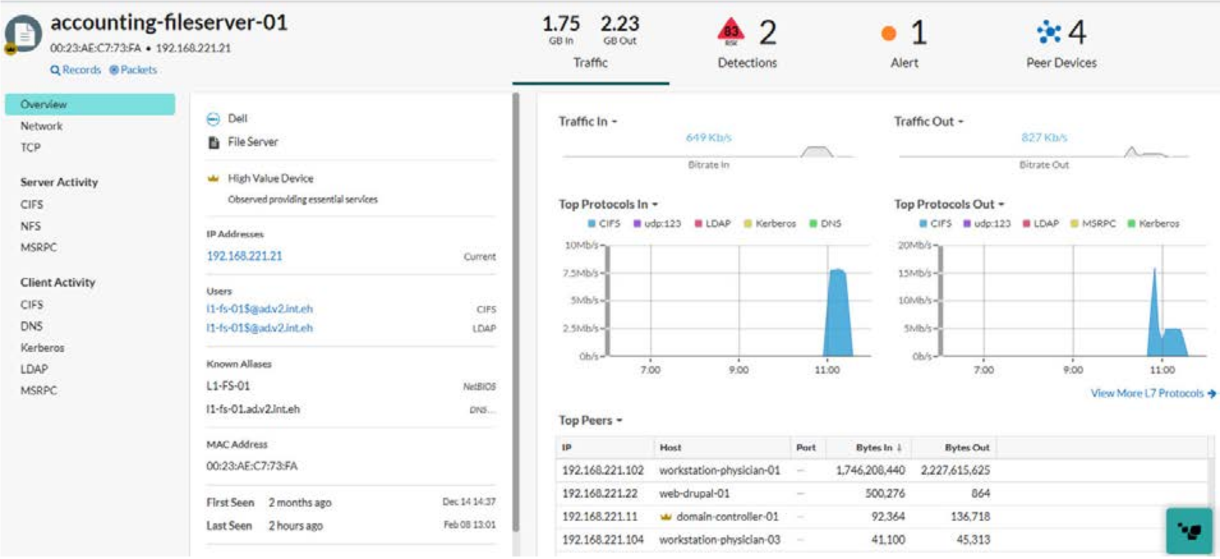
Devices by Role

Domain Controller	9 Devices
File Server	33 Devices
Mobile Device	1 Devices
PC	53 Devices
Vulnerability Scanner	0 Devices
VPN Client	0 Devices
VPN Gateway	1 Devices
Wi-Fi Access Point	0 Devices
IP Camera	0 Devices
Medical Device	0 Devices
Printer	1 Devices
VoIP Phone	54 Devices
Database	6 Devices
Web Server	39 Devices
Load Balancer	0 Devices
Web Proxy Server	0 Devices
Firewall	
Gateway	
Custom Device	
NAT Gateway	

Protocol			Map	Activity
AAA	40 servers	1 client		
CIFS	24 servers	88 clients		
Database	7 servers	14 clients		
DHCP	11 servers	74 clients		
DNS	29 servers	113 clients		
FTP	1 server	1 client		
HL7	1 server	2 clients		
HTTP	55 servers	131 clients		
ICA	7 servers	34 clients		
Kerberos	9 servers	67 clients		
LDAP	13 servers	76 clients		
MSRPC	20 servers	73 clients		
NFS	53 servers	7 clients		
NTLM	16 servers	36 clients		
RDP	1 server	1 client		
RTCP		50 devices		
RTP		50 devices		

Figure 12. Catalog of passively discovered devices, broken down by their roles, protocols, and activity

Each device is displayed in a clear and concise dashboard that serves as a starting point for performance and security investigations into that asset. The dashboard includes metadata such as the device's name, role, protocols, and other relevant information.



accounting-fileserver-01
00:23:AE:C7:73:FA • 192.168.221.21
Records Packets

1.75 GB In 2.23 GB Out Traffic
83 RISK 2 Detections
1 Alert
4 Peer Devices

Overview
Network
TCP

Server Activity
CIFS
NFS
MSRPC

Client Activity
CIFS
DNS
Kerberos
LDAP
MSRPC

Dell
File Server

High Value Device
Observed providing essential services

IP Addresses
192.168.221.21 Current

Users
l1-fs-01$@ad.v2.int.eh CIFS
l1-fs-01$@ad.v2.int.eh LDAP

Known Aliases
L1-FS-01 NetBIOS
l1-fs-01.ad.v2.int.eh DNS...

MAC Address
00:23:AE:C7:73:FA

First Seen 2 months ago Dec 14 14:37
Last Seen 2 hours ago Feb 08 13:01

Traffic In
649 Kb/s
Bitrate In

Traffic Out
827 Kb/s
Bitrate Out

Top Protocols In
CIFS udp:123 LDAP Kerberos DNS

Top Protocols Out
CIFS udp:123 LDAP MSRPC Kerberos

View More L7 Protocols

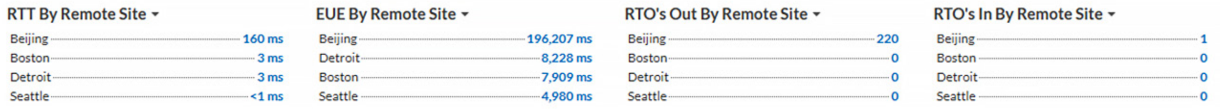
Top Peers

IP	Host	Port	Bytes In ↓	Bytes Out
192.168.221.102	workstation-physician-01	–	1,746,208,440	2,227,615,625
192.168.221.22	web-drupal-01	–	500,276	864
192.168.221.11	domain-controller-01	–	92,364	136,718
192.168.221.104	workstation-physician-03	–	41,100	45,313

Figure 13. Our user interface dynamically generates a dashboard for every device outlining it's entire profile, what users have touched it, application protocols it uses, active alerts, and much more - without any need for user input

Logical tracking of remote site traffic

With ExtraHop, ensuring the performance and reliability of datacenter services is a top priority. But it's also important to quickly identify and resolve network issues at branch offices and remote sites. ExtraHop provides a comprehensive view of network traffic by mapping client-to-server communication as its foundation. However, its versatility allows for data abstraction by application, device group, user, and even by specific remote locations and branch offices.



RTT By Remote Site	
Beijing	160 ms
Boston	3 ms
Detroit	3 ms
Seattle	<1 ms

EUE By Remote Site	
Beijing	196,207 ms
Detroit	8,228 ms
Boston	7,909 ms
Seattle	4,980 ms

RTO's Out By Remote Site	
Beijing	220
Boston	0
Detroit	0
Seattle	0

RTO's In By Remote Site	
Beijing	1
Boston	0
Detroit	0
Seattle	0

Figure 14. KPIs for remote site performance, broken down by site at an overview

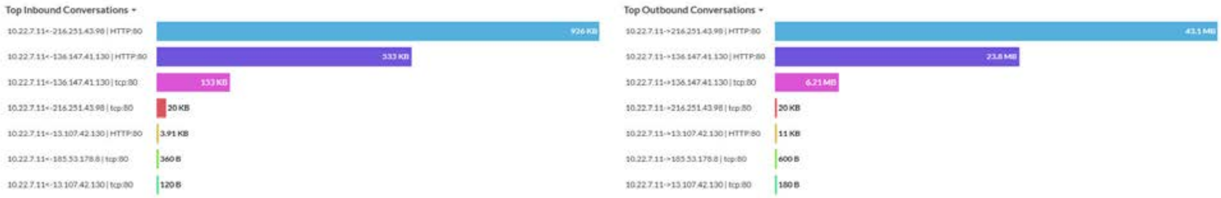
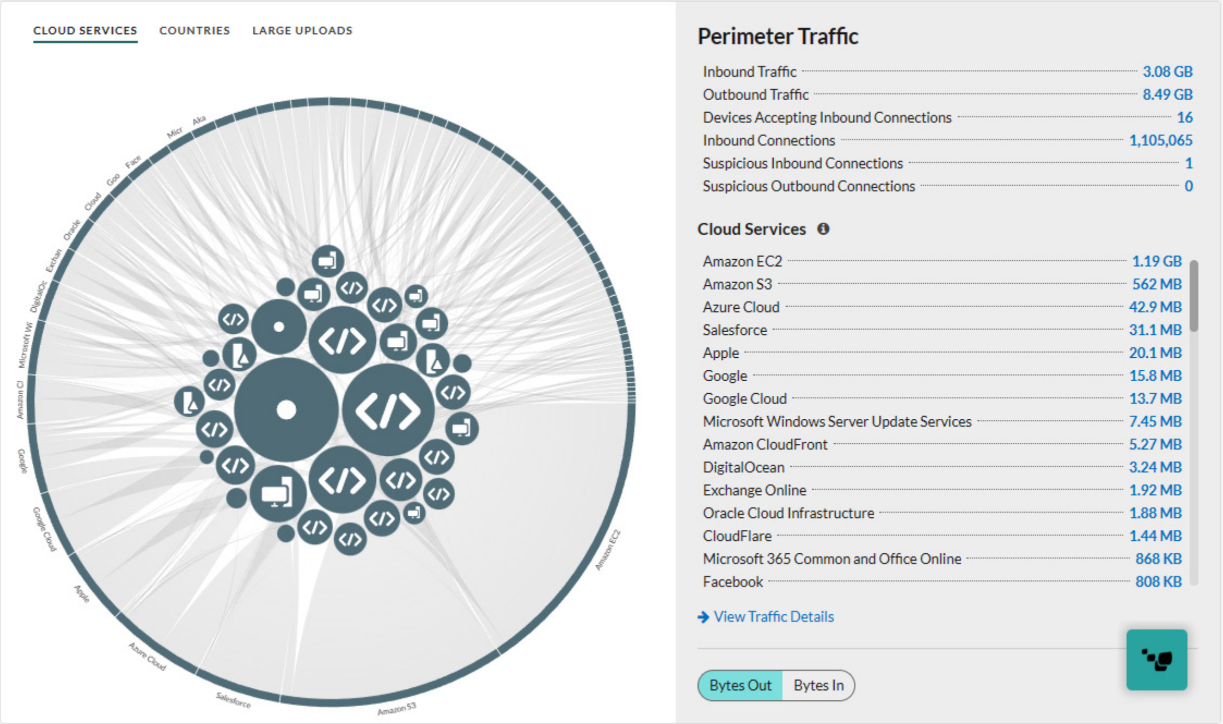


Figure 15. Drilling into a specific site reveals dozens of critical metrics for finding the source of bandwidth constraints, application slowness, and more

Cloud workloads, SaaS, and everything else

With the proliferation of public and private cloud services, including SaaS, PaaS, and IaaS, monitoring network performance has become increasingly complex. ExtraHop's solution offers comprehensive visibility, breaking down connections by service, traffic volume, and geographic location. Plus, with native sensors available for AWS, Azure, and GCP and seamless integration with on-prem sensors, you can have a unified view of your network performance through a single pane of glass.



Perimeter Traffic

Inbound Traffic	3.08 GB
Outbound Traffic	8.49 GB
Devices Accepting Inbound Connections	16
Inbound Connections	1,105,065
Suspicious Inbound Connections	1
Suspicious Outbound Connections	0

Cloud Services ℹ

Amazon EC2	1.19 GB
Amazon S3	562 MB
Azure Cloud	42.9 MB
Salesforce	31.1 MB
Apple	20.1 MB
Google	15.8 MB
Google Cloud	13.7 MB
Microsoft Windows Server Update Services	7.45 MB
Amazon CloudFront	5.27 MB
DigitalOcean	3.24 MB
Exchange Online	1.92 MB
Oracle Cloud Infrastructure	1.88 MB
CloudFlare	1.44 MB
Microsoft 365 Common and Office Online	868 KB
Facebook	808 KB

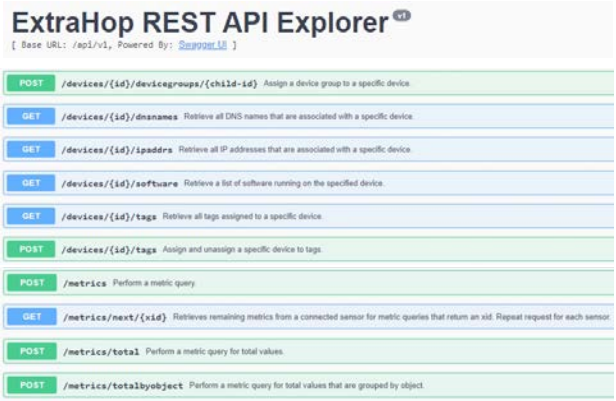
Figure 16. Analysis of all perimeter traffic (including cloud and SaaS destinations) entering or exiting the organization

Massive extensibility

Enterprise scale products need to fit the complex and ever expanding needs of the business. With native integrations to a range of IT and security tools, ExtraHop streamlines alert responses and facilitates collaboration between tools delivering compound interest on tool investments.

The full REST API grants access to all ExtraHop metrics, device metadata, and more. ExtraHop's internal trigger API empowers customers to build custom metrics and records through the trigger engine.

The potential for custom use cases and integration is nearly limitless.

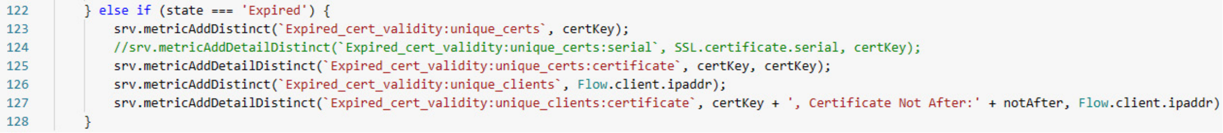


ExtraHop REST API Explorer v1

[Base URL: /api/v1, Powered By: Swagger UI]

POST	/devices/{id}/devicegroups/{child-id}	Assign a device group to a specific device.
GET	/devices/{id}/dnsnames	Retrieve all DNS names that are associated with a specific device.
GET	/devices/{id}/ipaddrs	Retrieve all IP addresses that are associated with a specific device.
GET	/devices/{id}/software	Retrieve a list of software running on the specified device.
GET	/devices/{id}/tags	Retrieve all tags assigned to a specific device.
POST	/devices/{id}/tags	Assign and unassign a specific device to tags.
POST	/metrics	Perform a metric query.
GET	/metrics/next/{xid}	Retrieves remaining metrics from a connected sensor for metric queries that return an xid. Repeat request for each sensor.
POST	/metrics/total	Perform a metric query for total values.
POST	/metrics/totalbyobject	Perform a metric query for total values that are grouped by object.

Figure 17. The REST API is well documented and viewable with a built-in Swagger API



```
} else if (state === 'Expired') {
    srv.metricAddDistinct(`Expired_cert_validity:unique_certs`, certKey);
    //srv.metricAddDetailDistinct(`Expired_cert_validity:unique_certs:serial`, SSL.certificate.serial, certKey);
    srv.metricAddDetailDistinct(`Expired_cert_validity:unique_certs:certificate`, certKey, certKey);
    srv.metricAddDistinct(`Expired_cert_validity:unique_clients`, Flow.client.ipaddr);
    srv.metricAddDetailDistinct(`Expired_cert_validity:unique_clients:certificate`, certKey + ', Certificate Not After:' + notAfter, Flow.client.ipaddr)
}
```

Figure 18. Trigger engine rules are created in standard Javascript with nearly unlimited use cases and detailed documentation for our classes and methods.

Conclusion

ExtraHop provides a comprehensive and sophisticated solution that supports a number of use cases for network traffic analysis, with a wide range of features that streamline the process of troubleshooting network issues, detecting security risks, and identifying compliance issues. Its powerful decoding capabilities and ability to quickly identify key performance indicators make it an invaluable tool for network professionals.

Additionally, ExtraHop's machine learning algorithms and passive asset discovery and classification provide insights into network behavior and performance that might otherwise be missed. With its massive extensibility and ability to integrate with a range of IT and security tools, ExtraHop is an enterprise-scale product that can be customized to fit the complex needs of businesses.

Seeing is believing. Try for yourself.

START DEMO

ABOUT EXTRAHOP NETWORKS

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The company's Reveal(x) 360 is the only network detection and response platform that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they see more, know more and stop more cyber attacks.

ExtraHop

info@extrahop.com
www.extrahop.com