



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...

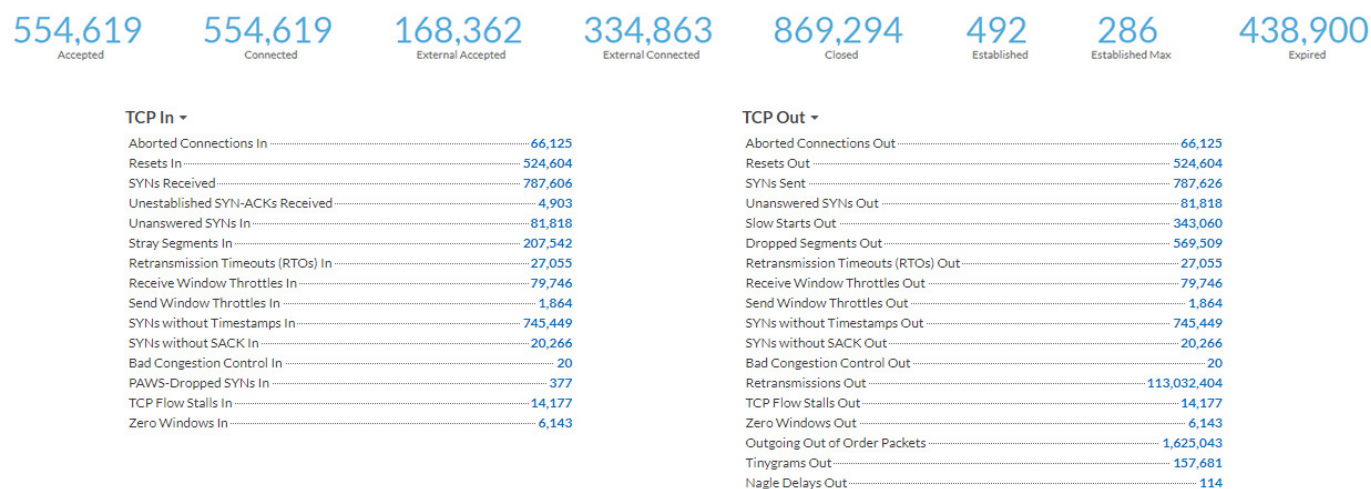


Figure 1. A sample of the metrics available in the ExtraHop platform for drilling into TCP performance

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.

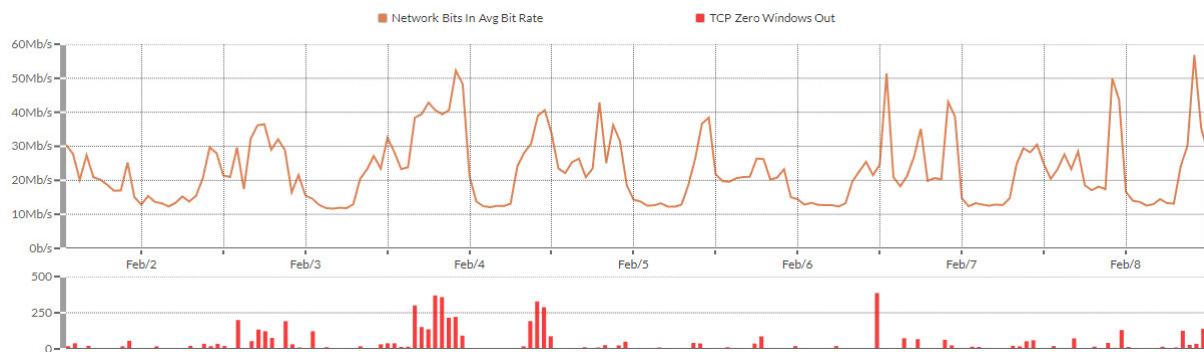


Figure 2. All metrics can be combined into charts and graphs for comparison, overlay, and analysis. These charts can be saved as dashboards for reports or on-demand viewing

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.

Database Response Time by Method ▾

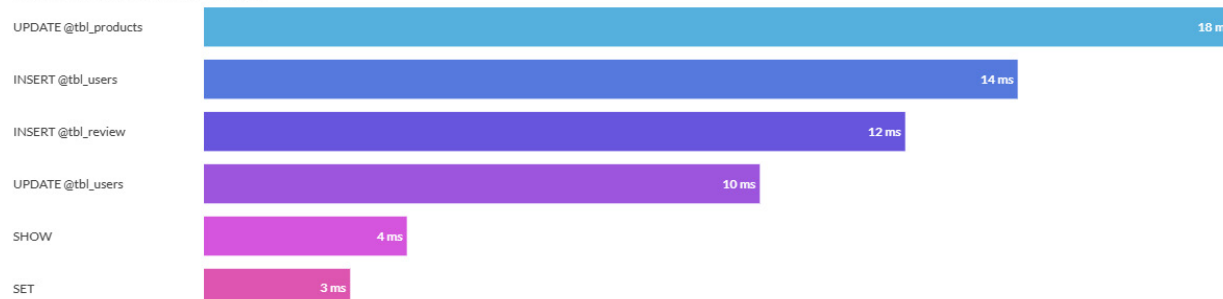
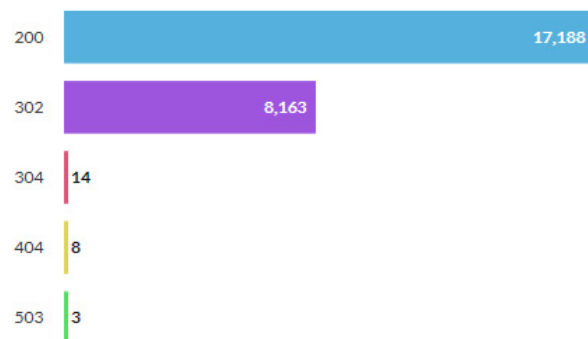


Figure 4. Finding a slow database transaction in a sea of servers, tables, and clients doesn't require logs or agents; it can be done instantly and passively from packets

End User Status Codes ▾



End User Server Processing Time By URI ▾

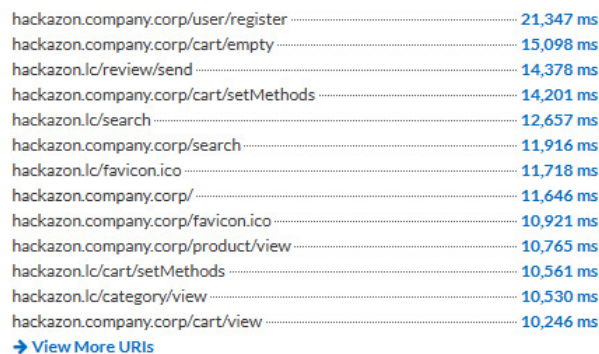


Figure 5. Web server errors, slowness, and unexpected behavior can be broken down to the URI level for rapid remediation

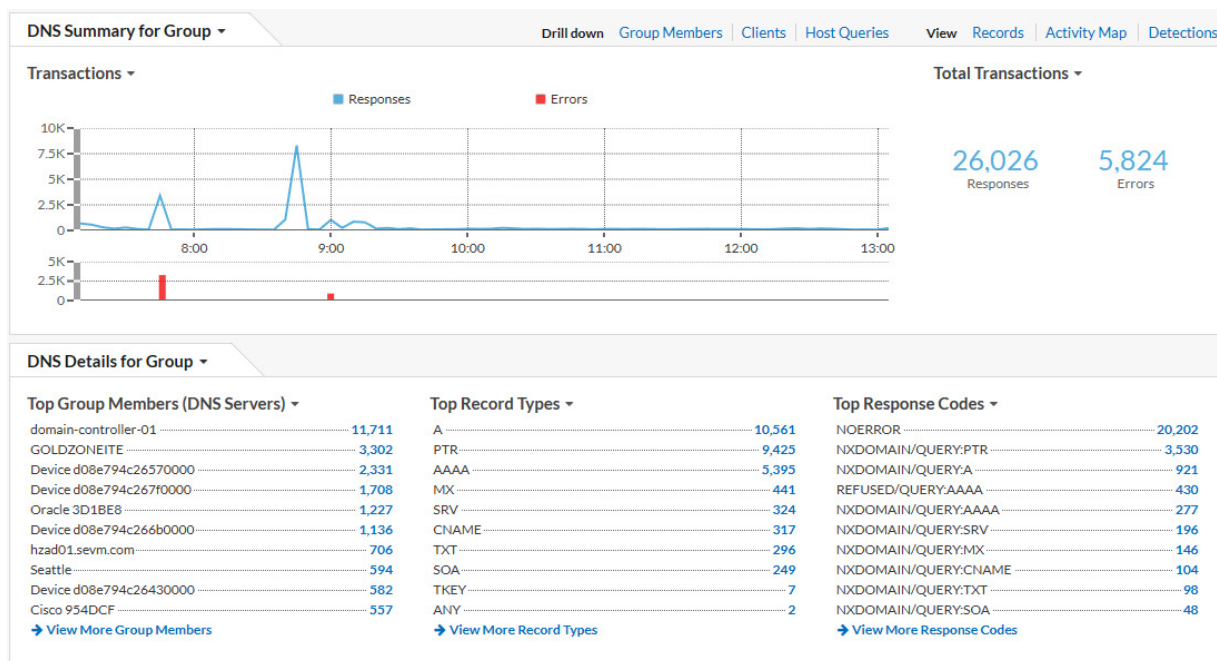


Figure 6. Other protocols like DNS, DHCP, and auth mechanisms are immensely important - ExtraHop can break all of these down and instantly spot spikes in errors for name resolutions, leases, and auth failures

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.

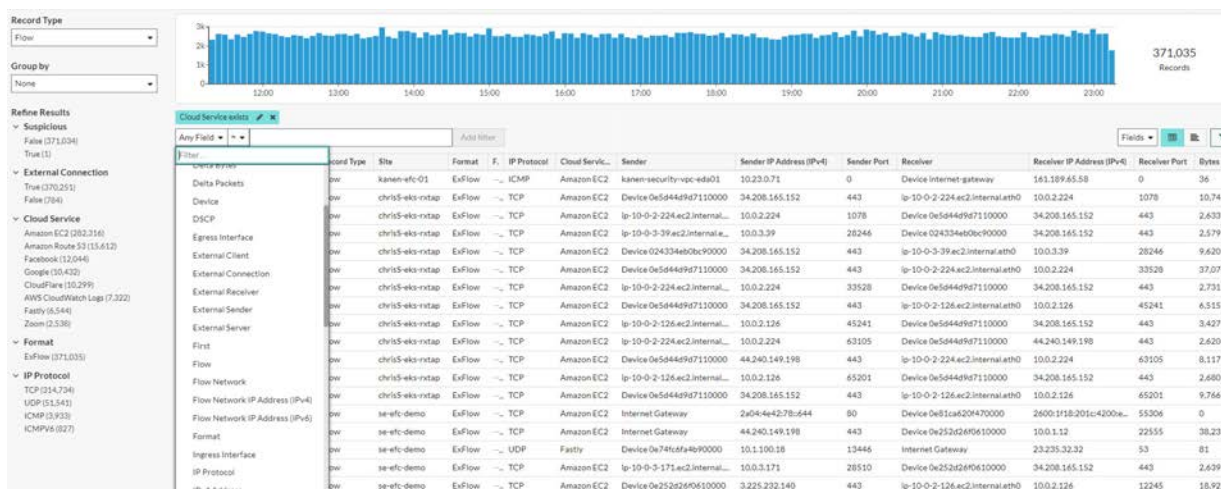


Figure 7. An example of a collection of flow records in the ExtraHop solution which can be filtered and searched using our powerful visual query language.

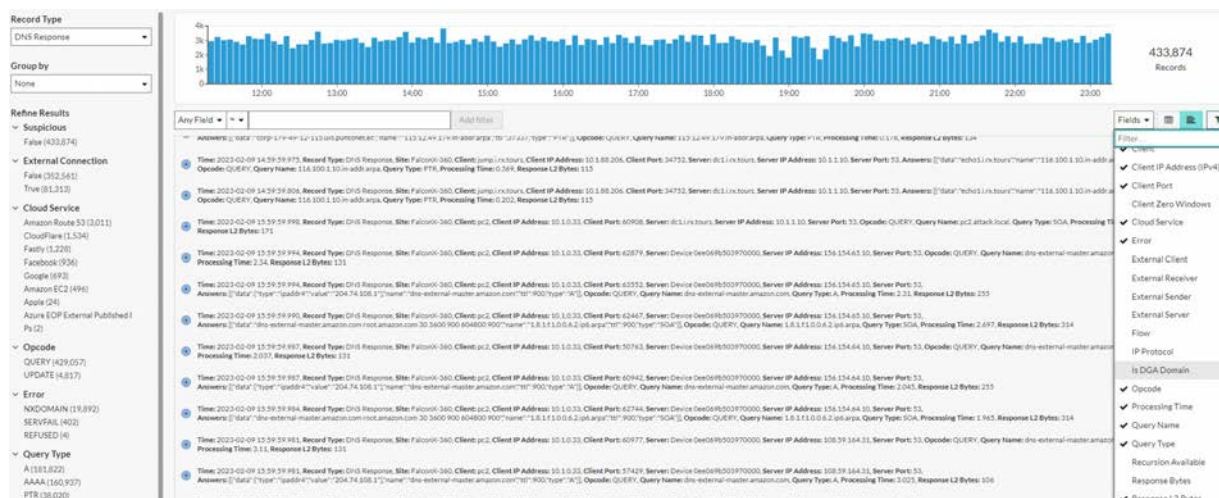


Figure 8. Records can show more detailed L7 protocols. Here is a sample of DNS transaction records.

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

Feb 8 09:00

lasting 34 minutes

CAUTION

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

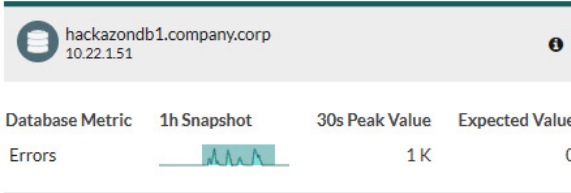


Figure 9. Application level error rates, latency, or anomalies are analyzed and alerts generated often before the performance impact is reported.

Delayed Data Transfer

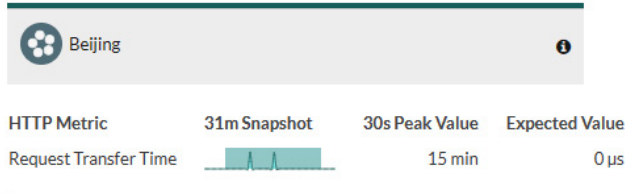
Feb 8 08:45

lasting 22 minutes

CAUTION

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



NEW OPER-7854 kpickles 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

CAUTION

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

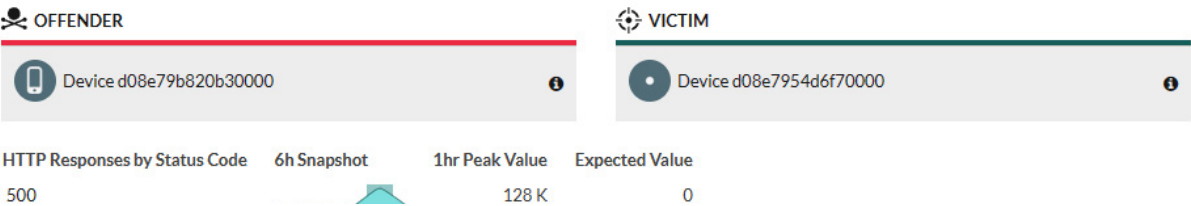


Figure 11. Web servers, applications, file delivery and other communications occur over web protocols like HTTPS.

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.

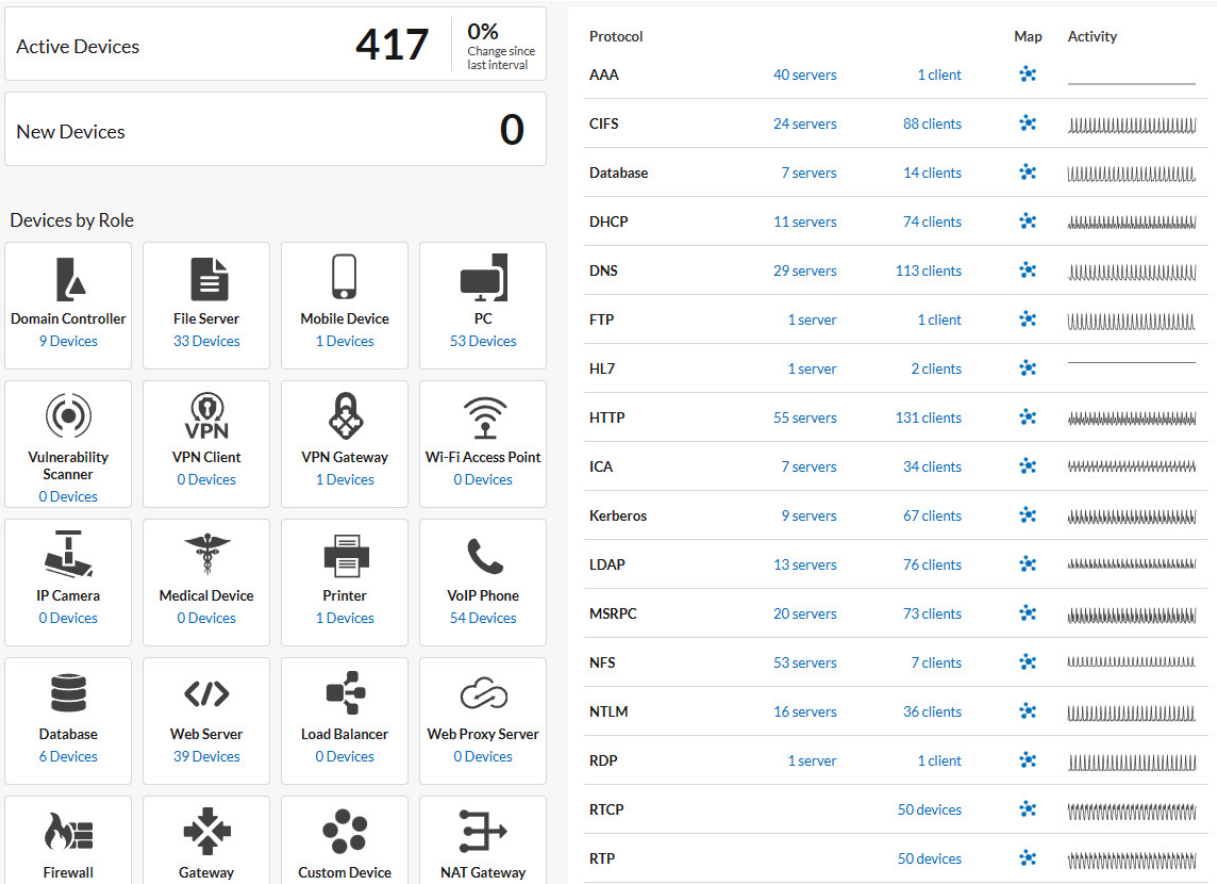


Figure 12. Catalog of passively discovered devices, broken down by their roles, protocols, and activity

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.

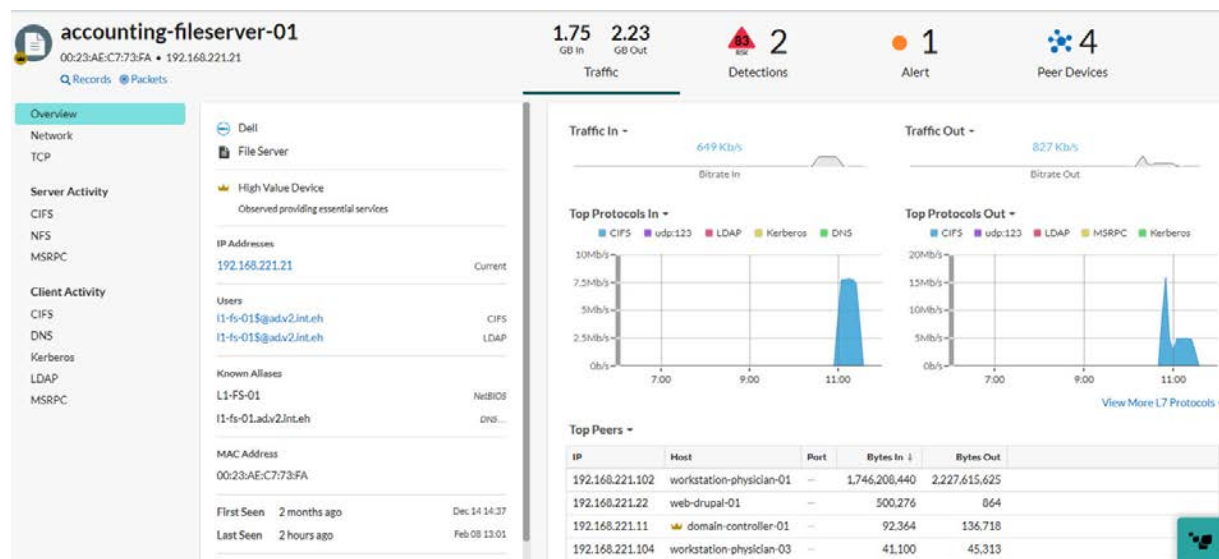


Figure 13. Our user interface dynamically generates a dashboard for every device outlining its entire profile, what users have touched it, application protocols it uses, active alerts, and much more - without any need for user input

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.

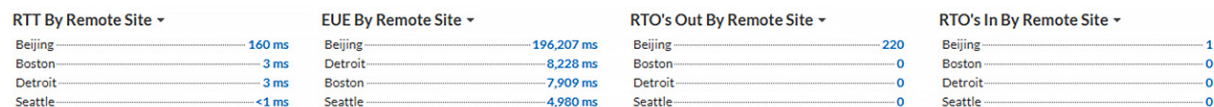


Figure 14. KPIs for remote site performance, broken down by site at an overview



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.

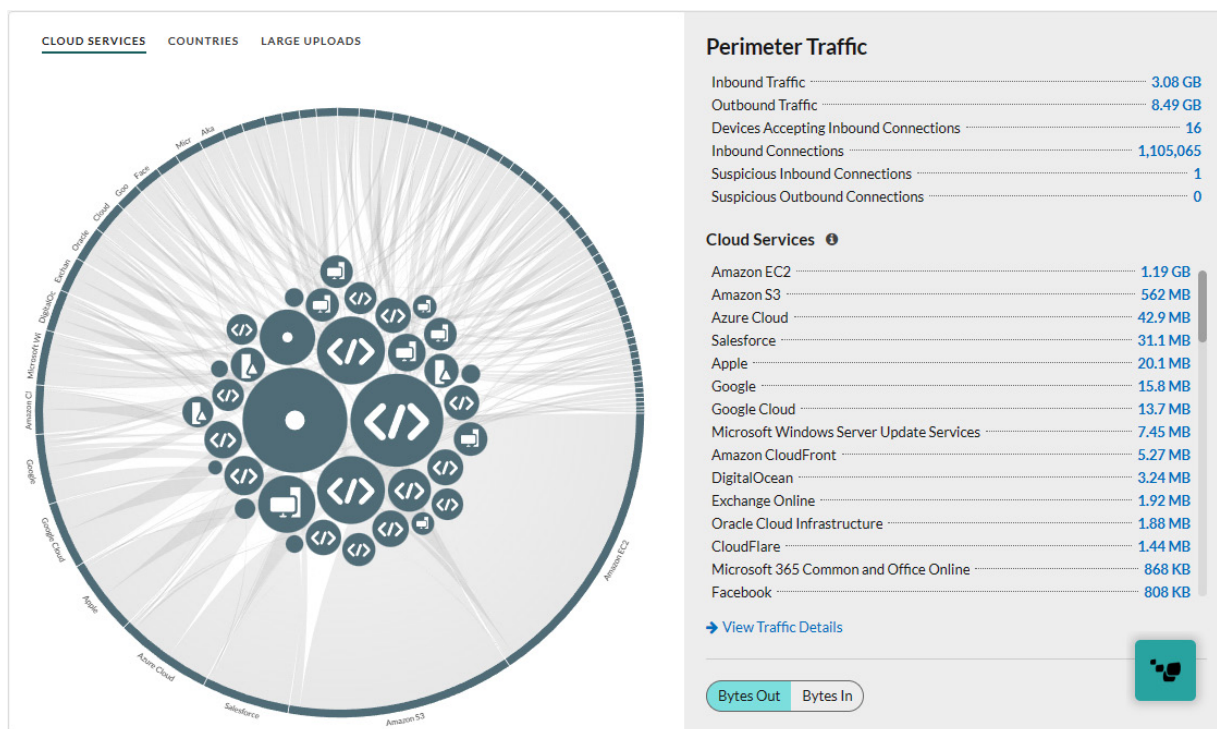


Figure 16. Analysis of all perimeter traffic (including cloud and SaaS destinations) entering or exiting the organization

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.

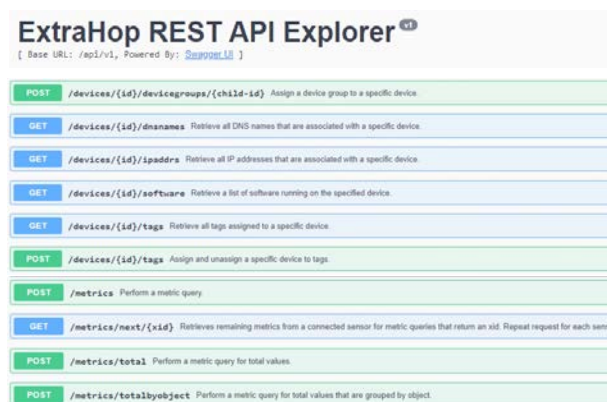


Figure 17. The REST API is well documented and viewable with a built-in Swagger API

```

122     } else if (state === 'Expired') {
123         srv.metricAddDistinct('Expired_cert_validity:unique_certs', certKey);
124         //srv.metricAddDetailDistinct('Expired_cert_validity:unique_certs:serial', SSL.certificate.serial, certKey);
125         srv.metricAddDetailDistinct('Expired_cert_validity:unique_certs:certificate', certKey, certKey);
126         srv.metricAddDistinct('Expired_cert_validity:unique_clients', Flow.client.ipaddr);
127         srv.metricAddDetailDistinct('Expired_cert_validity:unique_clients:certificate', certKey + ', Certificate Not After:' + notAfter, Flow.client.ipaddr)
128     }

```

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.



info@extrahop.com
www.extrahop.com