ExtraHop

WHITE PAPER

ExtraHop Platform Overview: Gain Control With Real-Time IT Analytics

Abstract

To overcome new challenges and achieve better outcomes, enterprise IT must rethink the network as a data source and not simply a means of transport. The ExtraHop platform unlocks the hidden value in the network, enabling IT, Security, and Business teams to mine all digital interactions for real-time insights. This paper explains why the network is the richest and most empirical data source, and how the ExtraHop platform enables data-driven operations.

Real-Time IT Analytics Starts with the Network

It's no secret that the IT landscape is evolving rapidly, creating new challenges for IT organizations. Megatrends such as mobility, desktop virtualization, ransomware, the Internet of Things, and the software-defined datacenter all demand that IT organizations operate smarter, equipped with real-time insights into what is happening in their environments. However, legacy IT monitoring products have not kept pace with these changes, leaving enterprises with a hodgepodge of niche tools designed for the paradigms of decades past. Left without a means to cut through increasing complexity, IT teams struggle to achieve key outcomes, including:

- **Consistent service delivery –** With more moving parts located in more places, it is no surprise that outages of business-critical applications regularly make news headlines. Downtime can be catastrophic. In today's digital businesses, employees, partners, and customers must have fast and reliable access to applications and data.
- **Protection of sensitive data –** In the realm of cybersecurity, not only are the barbarians at the gates, but they can scale the walls and steal what they want, seemingly at will. To detect suspicious behavior faster and mitigate risk, IT organizations are looking to improve their visibility into east-west traffic within the datacenter (lateral movement between servers).
- **Optimized user experiences –** Today, every interaction with customers depends on digital transactions occurring behind the scenes. Companies need to optimize these experiences to stay competitive and avoid embarrassing word-of-mouth complaints.
- **Keep up with the speed of business –** If everything stayed static, then IT organizations might stand a chance of catching up. The reality is that IT organizations increasingly play a critical role in a steady drumbeat of new initiatives tied directly to profits. They need to be able to support these new efforts quickly while minimizing risk and ensuring optimized experiences.

The ExtraHop platform offers a way forward, enabling IT organizations to fundamentally rethink their network as a data source, not just a means of transporting data. Industry-leading organizations such as Adobe, Alaska Airlines, Lockheed Martin, McKesson, Morgan Stanley, Nike, and Sony have already made this philosophical leap and rely on ExtraHop for real-time insights into application performance, cybersecurity risks, and business operations.

The Network Is the Richest Source of Data

As business continues to undergo digital transformation, the network has become the common denominator tying *everything* together. Consider the range of digital experiences that rely on communications over the network, from high-value activities such as booking an airline flight, paying bills online, and receiving medical care, to everyday activities such as ordering a lunch delivery or purchasing a concert ticket. Each of these digital experiences is supported by hundreds or even thousands of interactions between systems and devices on the network.

In the past, enterprises have treated the network simply as a delivery mechanism for these digital experiences. But what if you could mine the communications between devices for real-time insights and data-driven operations? That's exactly what ExtraHop makes possible. With the ExtraHop platform, IT organizations can unlock the hidden value in their networks, discovering, observing, and analyzing every digital interaction as it occurs.

Recognized Visionary in Network Performance Monitoring

In 2017 Gartner recognized ExtraHop in their Network Performance Monitoring and Diagnostics Magic Quadrant. This was the first time ExtraHop participated in this process. Although we are just now being recognized in this category, we've been helping organizations solve problems in the most complex and dynamic environments for almost 10 years.

ExtraHop is positioned as a visionary and placed furthest to the right for Completeness of Vision, which we believe is a testament to our focus on innovation and delivering the solutions customers need. We continue to build upon our position in this market by adding functionality like ExtraHop Addy, the first cloud service that applies machine learning to the richest source of IT data—wire data—to provide real-time situational insight for IT teams.

Figure 1. Magic Quadrant for Network Performance Monitoring and Diagnostics

Source: Gartner (February 2017)

Going Digital Brings New Challenges

The modern digital economy is comprised of millions of personal, business, and financial transactions and services happening in real time. There is a single common denominator enabling and facilitating the economy—it's the network. The network has been the common denominator of the information revolution for the past 30 years. However, the means to mine the valuable data from it has not fundamentally changed in over 20 years.

In order to keep up with the millisecond expectations of your business in today's digital economy, you need solutions that are real-time, scalable, multi-purpose, and usable across your organization.

However, making the transition from how things have always been done to a data-driven IT Analytics model can be challenging and requires having the right partner to provide the technology solutions and guidance to get there.

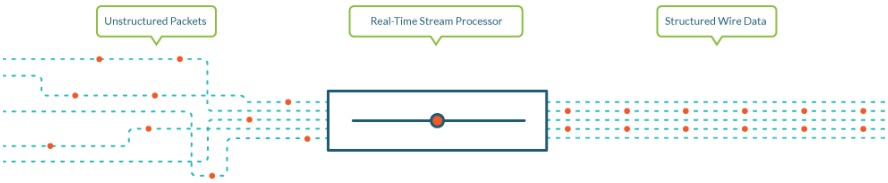
Change Doesn't Happen Overnight

ExtraHop recognizes organizations have existing workflows and provides a platform that can adapt to them, while also creating a bridge to the new era of IT Analytics. We take traditional network functions like packet capture and radically simplify and accelerate their workflows. When it comes to IT Operations and Security, ExtraHop can also simplify management of a solution and provide rich contextual data and an improved workflow for these roles with a pricing model that scales, instead of the traditional models which were defined by massive costs based on the data ingested.

All this is designed to make it easy to onboard ExtraHop in your environment, improve your organization's visibility, and reduce the friction on existing staff to ensure a successful transition from traditional NPM and APM to the world of IT Analytics. With the depth of data, the speed at which it can be translated into meaningful insights, and the ubiquitous nature of the data source, wire data is the first place forward-thinking IT teams look to solve problems in their environment.

From Network Packets to Wire Data

ExtraHop is an open, programmable, and extensible real-time streaming analytics platform that allows organizations to mine insights from all the data in motion within the IT environment. The ExtraHop platform analyzes a copy of network traffic from a port mirror or network tap, transforming unstructured packets into structured wire data at line rate, meaning that it can keep up with modern datacenter speeds. At the core of the product is a real-time stream processor that recreates TCP state machines for every client and server and then reassembles the complete sessions, flows, and transactions to extract L2 – L7 metrics. The resulting information is a crucial data source that Gartner Research calls wire data: "While log data will certainly have a role in future monitoring and analytics, it is Wire data — radically rethought and used in new ways — that will prove to be the most critical source of data for availability and performance management over the next five years."[1]



The ExtraHop platform performs full-stream reassembly, transforming unstructured packets into structured wire data and making sense of data in motion on the network.

Three Dimensions of Wire Data

The ExtraHop platform provides IT Operations, Security, and Business teams with the ability to access three different and complementary dimensions of their wire data.

- Metadata – Out of the box, the ExtraHop platform records 4,000+ metrics from the interactions it observes on the network. This metadata enables IT teams to view their entire IT environment and correlate behavior. For example, they can see that web response times increased as network congestion also rose—and then correlate that behavior with a storage backup process that was consuming network bandwidth and slowing down other applications. This type of global view of the entire IT estate is not possible with traditional types of monitoring tools and certainly not possible if your analysis is limited to packet captures.

- Transaction records – By indexing this metadata in a NoSQL datastore, the ExtraHop platform enables IT Operations and Security teams to perform multidimensional search and query functions for transaction records. This record search and query ability is familiar to IT Operations and Security because it is similar to what is provided by log indexing and analysis tools, except applied to transactions observed on the network instead of logs recorded by systems. Transaction records provide for a deeper level of investigation in the ExtraHop platform. For example, the user can search for all authentication requests for a particular account or see which users accessed a particular storage file.

- Packets – There is an old adage in IT: "Packets don't lie." When they need to prove something happened, IT and Security professionals rely on the actual packets to reconstruct an event or observed behavior. With packets, they have the digital forensic evidence they need to perform root-cause analysis or fulfill legal chain of custody requirements. They could prove to an application vendor that there is a bug in their software or prove an employee attempted to leak sensitive information, for example. In the ExtraHop platform, packets are available at the end of an investigation—in other words, after a user has identified an issue by looking at metadata and transaction records.

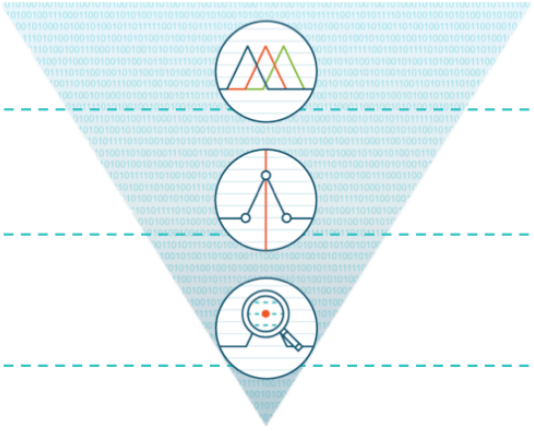
[1] Gartner, "Use Data- and Analytics-Centric Processes With a Focus on Wire Data to Future-Proof Availability and Performance Management," Vivek Bhalla and Will Cappelli, March 2016

	METADATA	TRANSACTION RECORDS	PACKETS
Use case	View the entire IT environment to create baselines, track trends, and identify issues early on	Use multidimensional query and search of transaction details to investigate and identify the root cause of an issue	Obtain the digital forensic evidence needed for root-cause analysis, legal prosecution, or as proof to third-parties
How it works	Stream processing and full-stream reassembly	Indexed NoSQL datastore	Continuous packet capture
ExtraHop Appliance	ExtraHop Discover (EDA)	ExtraHop Explore (EXA)	ExtraHop Trace (ETA)

Enabling Natural and Rapid Workflows

Traditionally, IT Operations, Network, and Security teams have relied on packet capture technologies to derive insight off of the network. In this approach, packets are recorded directly to storage and then analyzed later using a packet analysis tool such as Wireshark. Only experienced network and security engineers are trained to interpret this data, which is regarded as the most granular and empirical evidence that something happened.

The ExtraHop platform turns this approach on its head. Instead of analyzing only a small segment of network traffic after it has been recorded to disk, the ExtraHop platform analyzes network traffic as it passes over the network and then records the key insights—web errors, login failures, database methods used, files transferred, transaction IDs, and much more—in a format that everyone can understand. This analysis of data in motion as opposed to data at rest is crucial, because it enables much more natural and rapid workflows for IT Operations and Security professionals, as shown in the illustration below. With ExtraHop, IT professionals can complete key workflows in a matter of clicks, not hours.

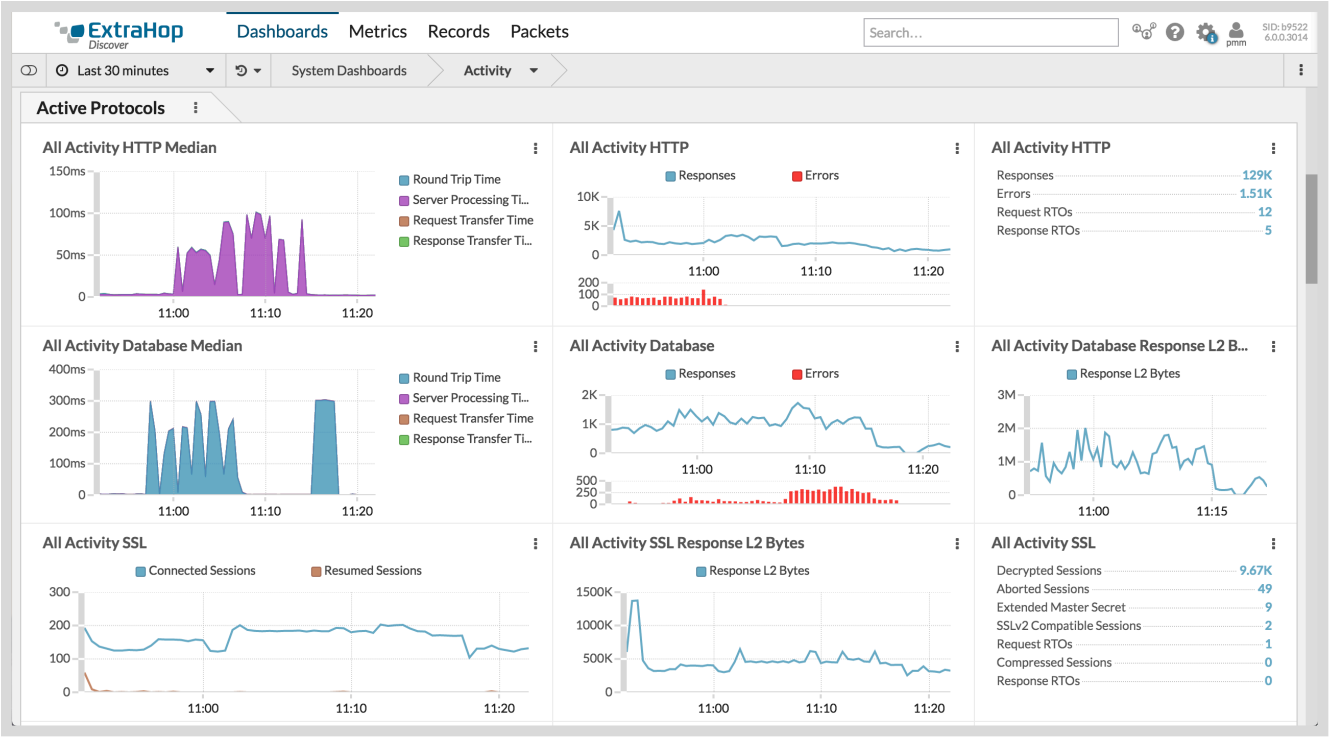


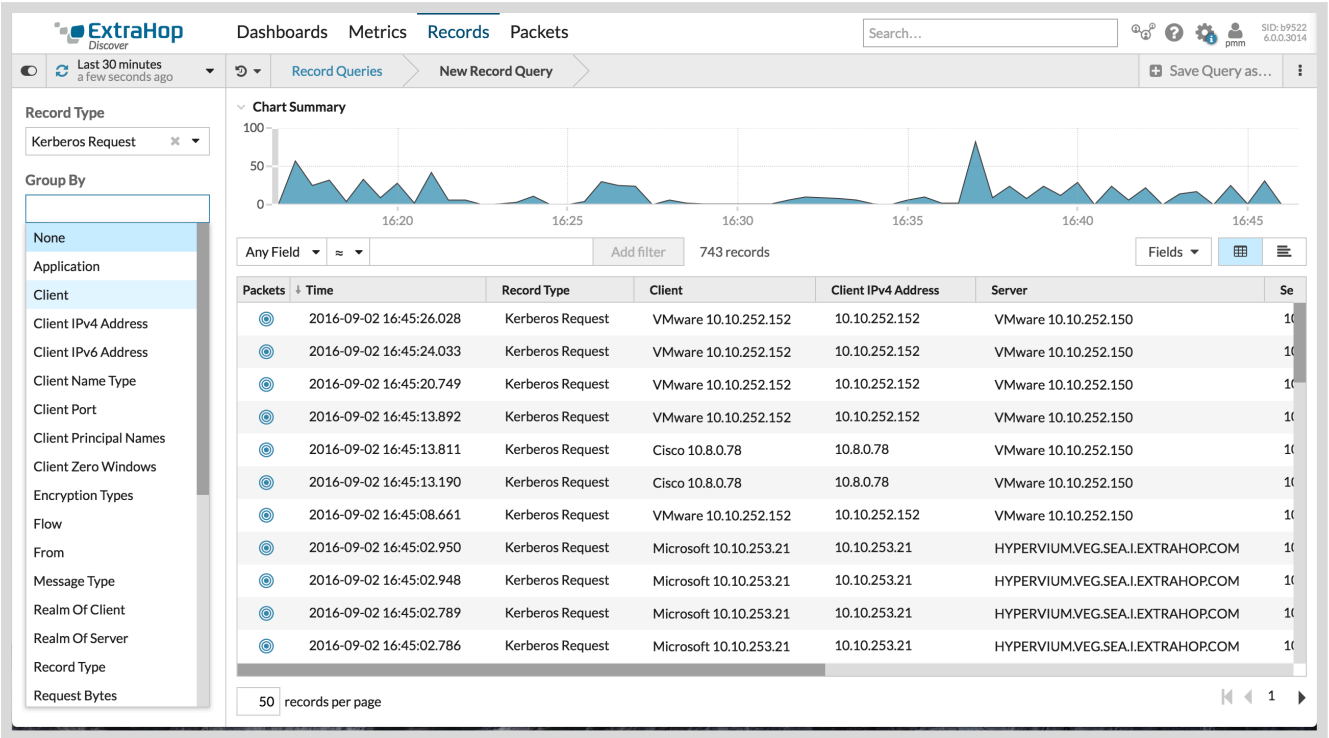
Discover the Entire Picture – Gain a comprehensive, global, and real-time view of everything transacting on the wire.

Explore Every Interaction – Get the granular, indexed, and searchable details of every transaction.

Trace Down the Details – Drill down to, or begin with, the individual metrics, users, or packets.

ExtraHop equips organizations to understand what is happening in their environment and investigate details, cutting complexity and enabling data-driven operations. Within five clicks or less, users can drill down from high-level dashboards to see transaction records and then download the packets that comprise those transactions.


ExtraHop Discover
Dashboards
Metrics
Records
Packets
Search...
Last 30 minutes
System Dashboards
Activity
Active Protocols
All Activity HTTP Median
150ms
100ms
50ms
0
11:00
11:10
11:20
Round Trip Time
Server Processing Ti...
Request Transfer Time
Response Transfer Ti...
All Activity HTTP
Responses
Errors
10K
5K
0
200
100
0
All Activity HTTP
Responses 129K
Errors 1.51K
Request RTOs 12
Response RTOs 5
All Activity Database Median
400ms
300ms
200ms
100ms
All Activity Database
2K
1K
500
250
All Activity Database Response L2 B...
Response L2 Bytes
3M
2M
1M
11:15
All Activity SSL
Connected Sessions
Resumed Sessions
300
200
100
All Activity SSL Response L2 Bytes
1500K
1000K
500K
All Activity SSL
Decrypted Sessions 9.67K
Aborted Sessions 49
Extended Master Secret 9
SSLv2 Compatible Sessions 2
Request RTOs 1
Compressed Sessions 0
Response RTOs 0

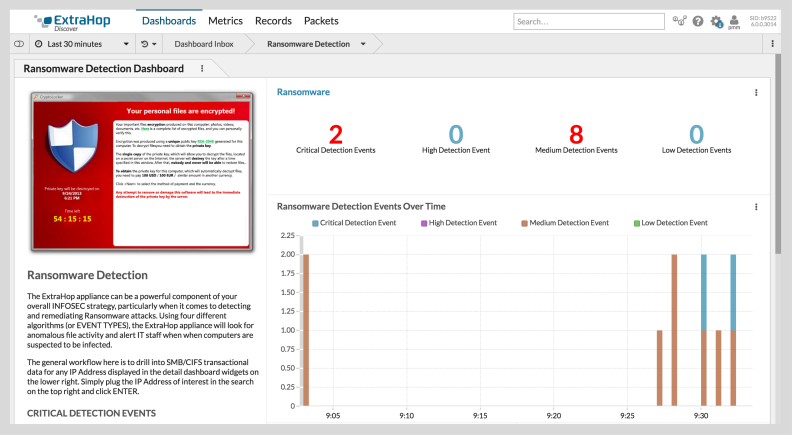

ExtraHop Discover
Dashboards
Metrics
Records
Packets
Search...
Last 30 minutes
a few seconds ago
Record Queries
New Record Query
Save Query as...
Record Type
Kerberos Request
Group By
None
Application
Client
Client IPv4 Address
Client IPv6 Address
Client Name Type
Client Port
Client Principal Names
Client Zero Windows
Encryption Types
Flow
From
Message Type
Realm Of Client
Realm Of Server
Record Type
Request Bytes
Chart Summary
100
50
0
16:20
16:25
16:30
16:35
16:40
16:45
Any Field
Add filter
743 records
Fields
Packets
Time
Record Type
Client
Client IPv4 Address
Server
2016-09-02 16:45:26.028 Kerberos Request VMware 10.10.252.152 10.10.252.152 VMware 10.10.252.150
2016-09-02 16:45:24.033 Kerberos Request VMware 10.10.252.152 10.10.252.152 VMware 10.10.252.150
2016-09-02 16:45:20.749 Kerberos Request VMware 10.10.252.152 10.10.252.152 VMware 10.10.252.150
2016-09-02 16:45:13.892 Kerberos Request VMware 10.10.252.152 10.10.252.152 VMware 10.10.252.150
2016-09-02 16:45:13.811 Kerberos Request Cisco 10.8.0.78 10.8.0.78 VMware 10.10.252.150
2016-09-02 16:45:13.190 Kerberos Request Cisco 10.8.0.78 10.8.0.78 VMware 10.10.252.150
2016-09-02 16:45:08.661 Kerberos Request VMware 10.10.252.152 10.10.252.152 VMware 10.10.252.150
2016-09-02 16:45:02.950 Kerberos Request Microsoft 10.10.253.21 10.10.253.21 HYPERVIUM.VEG.SEA.I.EXTRAHOP.COM
2016-09-02 16:45:02.948 Kerberos Request Microsoft 10.10.253.21 10.10.253.21 HYPERVIUM.VEG.SEA.I.EXTRAHOP.COM
2016-09-02 16:45:02.789 Kerberos Request Microsoft 10.10.253.21 10.10.253.21 HYPERVIUM.VEG.SEA.I.EXTRAHOP.COM
2016-09-02 16:45:02.786 Kerberos Request Microsoft 10.10.253.21 10.10.253.21 HYPERVIUM.VEG.SEA.I.EXTRAHOP.COM
50 records per page
1

Gain Control to Achieve Better Outcomes

By unlocking the hidden value in the network, the ExtraHop platform enables organizations to cut complexity and regain control. With ExtraHop, IT Operations, Security, and Business teams can detect every digital interaction, observe all activity in real time, and apply analytics for data-driven decisions.

Dynamic Discovery

In today's fast-changing IT environments, automatic discovery and classification is an absolute requirement for any monitoring platform. As the management axiom states: "You can't manage what you can't measure." Whereas traditional solutions require IT teams to tell them what to monitor, the ExtraHop platform automatically discovers devices, applications, and users communicating on the network. This continuous, passive observation of all network activity is especially of value for security operations, which currently lack real-time visibility into east-west communications between servers inside the datacenter.



With ExtraHop, Security Operations teams can automatically discover activity that represents risk, such as ransomware, and orchestrate automatic responses with REST API calls to firewall and network access control appliances.

Automatic device and application discovery is also critical when mapping application dependencies. Many ExtraHop customers use the platform to discover what is actually in their environment before migrating applications or after a merger or acquisition. Upon deploying ExtraHop, one large enterprise was surprised to find that the number of devices acting as DNS servers was several times more than they had documented. IT teams frequently benefit from ExtraHop's automatic discovery capability by identifying unauthorized use of service accounts, Shadow IT applications, or servers that were thought to have been decommissioned.

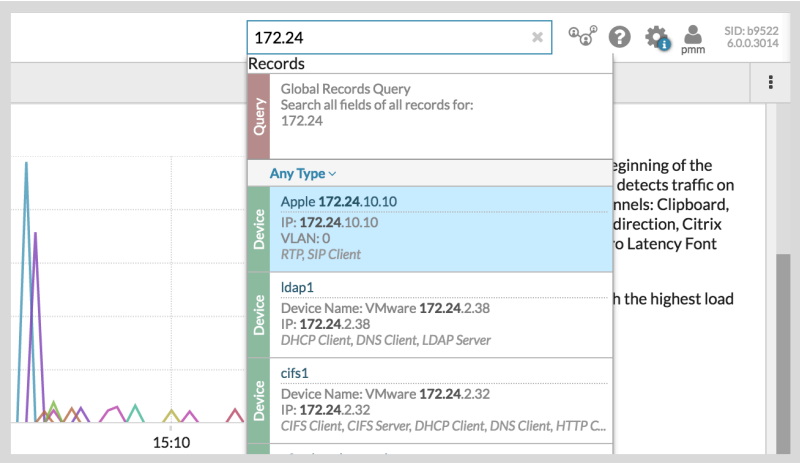
Universal Observation

The ExtraHop platform requires no agents installed on clients or servers, but instead passively observes all digital interactions occurring on the network. This continuous observation enables IT, Security, and Business users to explore the behavior of a specific device, application, or user both in real time and over a specified time period. Machine learning identify anomalous behavior, enabling IT teams to quickly fix problems before they impacts users, Security teams to detect activities that represent risk, and Business teams to understand how their digital businesses are performing.

In addition to real-time observation, the ExtraHop platform also enables organizations to look back in time and observe trends and activity. Users can easily perform a global search for a specific user name, IP address, URL, file name, or other element and then pivot and filter on the data to answer questions, such as "Which user agents (browser and operating system) have the best and worst performance on our site?" or "How many other clients downloaded the same malware?" or "What other files did this user delete off of the file share?" or "Which servers are using cipher suites with 1,024-bit encryption keys?"

Global search facilitates rapid, bottom-up workflows. Users can start from an IP address, user name, file name, or even the text in an error message.

The unified interface offers a seamless experience as users navigate between summary metrics, transaction records, and packet details.



Actionable Analytics

The ExtraHop platform enables IT organizations to mine digital interactions for insights. While other products that use the network as a data source provide esoteric information about the performance of the network itself, ExtraHop makes it possible for non-specialists to gain rapid insights from the richest and most empirical data source available—their network. Most ExtraHop customers remark that this ability to share visibility across teams has eliminated finger-pointing, improved collaboration, and made truly data-driven decisions possible.

A single ExtraHop Discover appliance can process up to 40 Gbps of sustained network traffic, which amounts to 432 TB of information each day for a fully saturated network link. This is Big Data analysis, but without the big management headache or a massive footprint. Better still, users do not need to be data scientists to understand what they see in ExtraHop. In addition, the Open Data Stream capability enables enterprises to stream any metrics or events from ExtraHop into third-party platforms for correlation with other data sets such as logs and security events.

Conclusion

It is time for enterprise IT to rethink the network as a data source, not just a means of transport. The ExtraHop platform represents a simple, elegant, and scalable way for organizations to take advantage of the richest data source available—their network. Leading companies in retail, healthcare, technology, financial services, and other industries rely on the ExtraHop platform for data-driven operations. By mining the digital interactions on their network, these organizations are cutting through complexity and achieving better outcomes: Consistent service delivery, reduced security risk, optimized user experiences, and greater agility.

About ExtraHop
ExtraHop makes real-time data-driven IT operations possible. By harnessing the power of wire data in real time, network, application, security, and business teams make faster, more accurate decisions that optimize performance and minimize risk. Hundreds of organizations, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google, start with ExtraHop to discover, observe, analyze, and intelligently act on all data in flight on-premises and in the cloud.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA

www.extrahop.com
info@extrahop.com