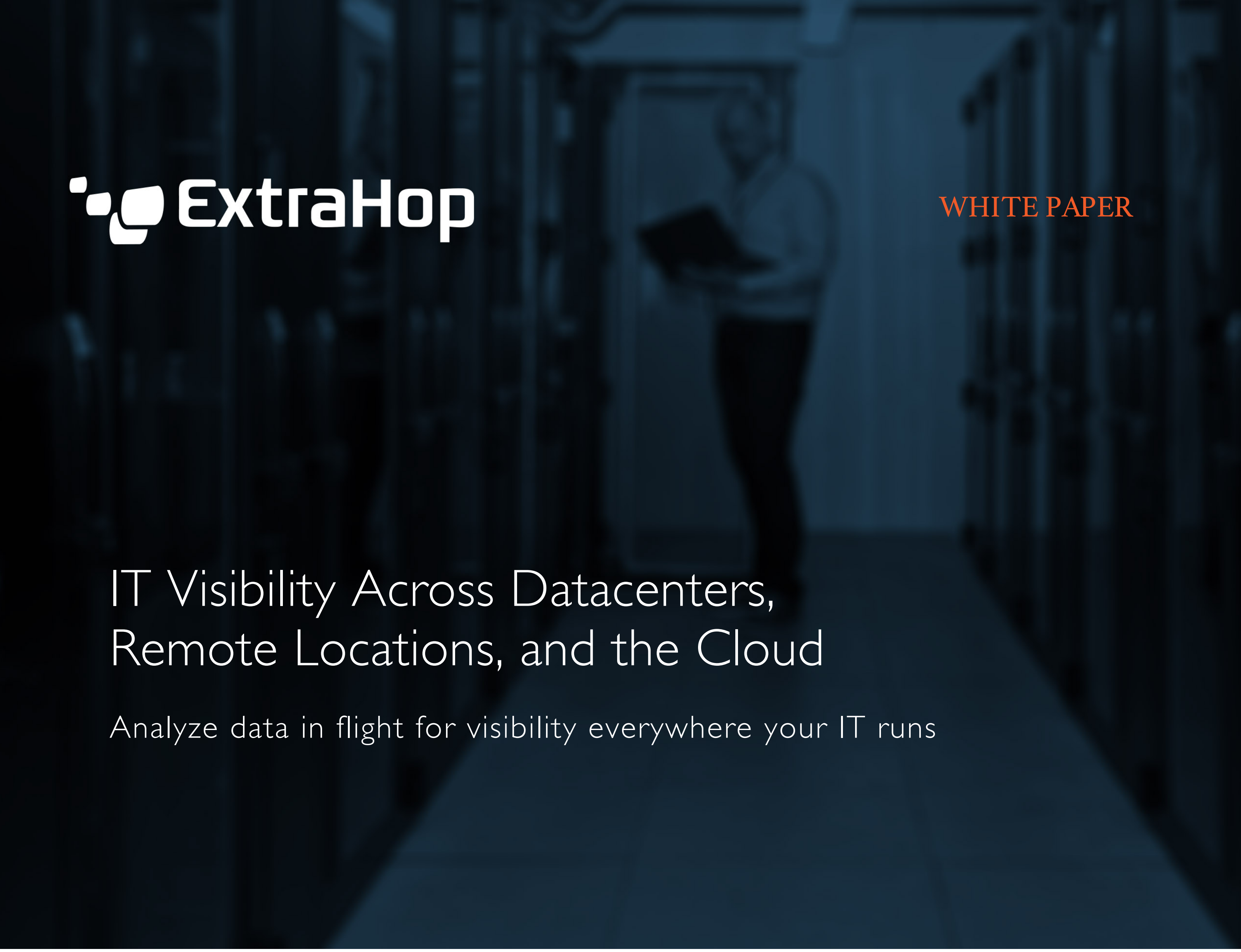


WHITE PAPER

IT Visibility Across Datacenters, Remote Locations, and the Cloud

Analyze data in flight for visibility everywhere your IT runs

Abstract

IT organizations are being asked to support applications and infrastructures across diverse and distributed environments, but traditional monitoring tools are not up to the task. As a result, IT organizations are working harder, but still not delivering the performance and security that is required. The network is the one constant that can offer insight into every device and applications in your datacenter, in a private or public cloud, or in dozens of remote offices. The ExtraHop platform analyzes all your data in flight so that you have the real-time insights needed to confidently control IT assets and infrastructure in diverse and geographically distributed environments.

Diverse, Sprawling IT Environments

Every organization today relies on technology to get business done—whether to assist in designing the next breakthrough product, schedule and report on field services engagements, or ring up a customer in a store. These interactions between IT and core business activities are often what determine the success or failure of the broader organization. This means that IT Operations teams need to be able to monitor and manage applications and infrastructure wherever these things happen. With more machines and applications located in far-away branch offices or in the cloud, IT Operations teams find themselves increasingly pressured to maintain their availability, performance, and security objectives. No matter where IT runs, there is still a need to be able to discover new devices and applications, observe their activity, and analyze that information for real-time insights.

The problem is that yesterday's IT monitoring and management tools are not built to provide real-time visibility across geographically dispersed environments. IT organizations have enough trouble keeping their traditional enterprise monitoring frameworks up and running in the corporate datacenter, not mention extending those solutions to remote offices, SaaS applications, and the public cloud. As a result, Operations teams "make do" with built-in monitoring tools such as WMI (Windows Management Instrumentation) or AWS CloudWatch that report basic resource-utilization metrics and cobble together a collection of disjointed tools that provide patchwork visibility into their operations.

Outdated monitoring approaches limit visibility and cause Operations teams to guess when it comes time to plan capacity and troubleshoot performance issues, not to mention ensure the security of new IT assets and infrastructure. They also fail to provide any operational or business analytics for what goes on at these distributed locations. The result is wasted capacity, unhappy users, uninformed business owners, and a demoralized IT team that does not have the visibility needed to do their job correctly.

IT Operations teams are responsible for a variety of distributed environments, ranging from datacenters to personnel in the field.

The Network to the Rescue

What if there was a single point of instrumentation that could provide both meaningful insight and worked in every type of environment? The good news is that you have had a constant, uniform source of real-time insight all along: your network! No matter whether the devices and applications you are tasked with supporting runs in your datacenter, in the cloud, or in dozens of remote offices, it will communicate on the network. The answer to managing IT in diverse and geographically distributed environments lies in making sense of all that rich data in flight.

With ExtraHop you can gain control over hybrid IT environments and geographically-distributed deployments. Instead of relying on deploying agents or gathering logs, ExtraHop delivers insights from all data in flight via data observed on the network. This type of deployment works anywhere—the only thing that IT needs to worry about is getting the traffic to an ExtraHop appliance. Because you get a centralized view, you can extend IT and business visibility in a way that's never been possible until now.

Distributed Deployment, Centralized Visibility

In the ExtraHop deployment model, data is processed at the edge, close to where it is generated (from the network tap or port mirror). This model minimizes data transport costs in geographically distributed environments and also facilitates faster access to real-time data compared with traditional monitoring solutions.

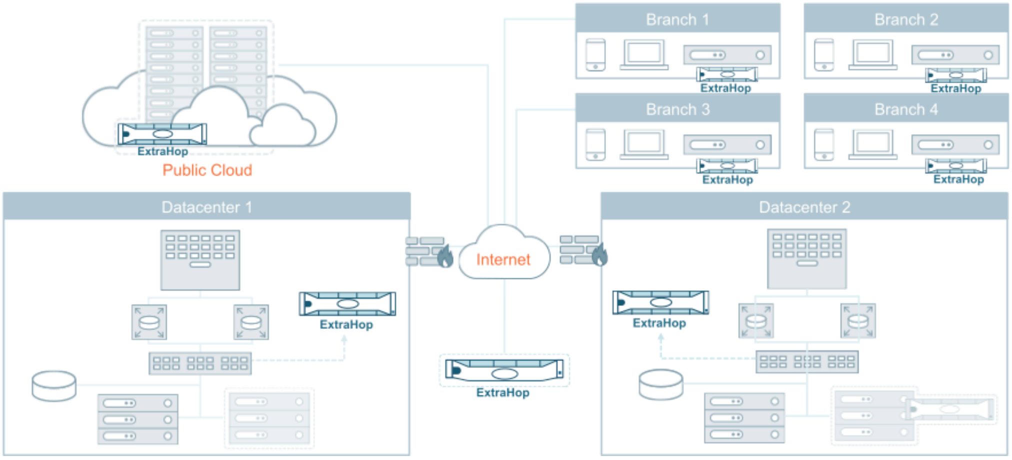
The ExtraHop Discover appliance (EDA) is available in a number of appliance types so that you can deploy them wherever your IT runs: in the public cloud, in heavily virtualized converged environments, in traditional on-premises datacenters, or in remote offices or retail stores.

ExtraHop Discover Appliance Types			
Physical rack-mounted 2U and 1U appliances that are appropriate for datacenters and large environments.	Small form factor Compact device that can be mounted on a wall or shelf in an "IT closet."	Virtual appliances VMware, Hyper-V, and KVM appliances for when more flexibility is needed.	Cloud appliances AWS- and Azure-ready appliances to bring visibility to your cloud environments.

Operations personnel can see across the entire IT estate by accessing the web UI of a central manager, the ExtraHop Command appliance. The ExtraHop Command appliance aggregates and unifies the visibility provided by the EDA nodes, making it possible to manage your disparate environments with a common view. This central management technology scales across hundreds of distributed EDA nodes, as proven by ExtraHop's own Atlas reports remote analysis service.

Defying Data Gravity

In the field of Big Data, there is a concept called "data gravity." The concept has many implications, but some of the key takeaways are that it is expensive to move data and that data is more valuable when it's together with other contextual data. Applied to the problem of monitoring geographically distributed IT environments, the concept of data gravity means that traditional forms of monitoring such as logging and SNMP polling become much more expensive as the number of distributed sites grows, as that data needs to be sent to a central server for analysis. In contrast, the ExtraHop deployment model analyzes data very close to where it is created—off the network—and so minimizes data transport costs.



The ExtraHop Command appliance (ECA) provides an aggregated and unified view across hundreds of ExtraHop Discover appliance (EDA) nodes in different environments.

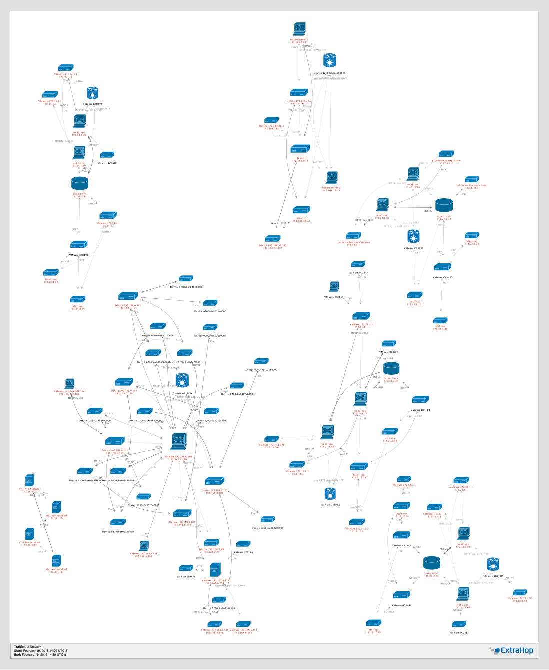
> "We used ExtraHop to pinpoint the cause of a slowdown for one of our 12 eClinicalWorks EHR deployments that our ambulatory clinics use, which was due to how our production and replica databases were racked in our datacenter. It was not an easy thing to diagnose—all we could see was that there were lots of timeouts and just overall a bad user experience. ExtraHop provided the critical information we needed to not only solve the problem but prevent it from happening again."
>
> ***Mat Demers, Director of Systems Engineering, Steward Health Care***

Automatically Discover Every Device and Application

If a device or application communicates on the network, then the ExtraHop platform automatically discovers and classifies it. This is important because IT Operations teams often do not have a complete or up-to-date inventory of the IT assets running in a remote office or newly acquired datacenter. ExtraHop can give them an automatically updated view of all the devices and applications that are communicating on the network.

The adage "You cannot manage what you cannot measure" applies here. IT Operations teams need insight into what devices and applications are active in their environments before they can make decisions about decommissioning, consolidation, or adding capacity. The ExtraHop platform provides the visibility needed to make these decisions, including the dependencies between servers or applications that may not show up on manually updated documentation or spreadsheets.

The ability to see new devices and activity is especially important when it comes to security. Decentralized IT broadens the "attack surface" that InfoSec and IT teams are responsible for defending. In branch offices or out in the field, attackers may be able to more easily gain physical access to IT assets making them even more vulnerable. The ExtraHop platform makes it possible for these security-minded teams to constantly be up-to-date about what devices and applications that are active in their environment. InfoSec teams will be able to see when a remote office has set up their own database or file server, for example. With ExtraHop, you can develop an InfoSec visibility strategy to complement your existing security toolset and improve the security posture of the organization.



Application Activity Maps help when making IT management decisions and identifying assets that need to be managed.

Observe Activity in Every Environment

Yesterday's resource-utilization metrics won't cut it when you are trying to troubleshoot application performance issues in today's virtualized, microservices-oriented, and container-based paradigms. You need deep and broad visibility across tiers, which is exactly what ExtraHop delivers with its stream analytics platform.

With the ability to observe real-time activity at a granular level, you can more easily identify not only which remote sites are seeing slow performance, but also what is going on inside their environment that might be affecting their experience. For SaaS applications, the ExtraHop platform enables you to objectively determine whether latency is due to network transfer time or slowness on the part of the SaaS provider.

In the public cloud, the ExtraHop platform provides unprecedented transaction-level visibility for applications. This facilitates applications migrations to the cloud because application owners can measure performance before, during, and after the migration. For example, in Amazon Web Services, IT teams can see how workloads perform across AWS Regions and make more informed EC2 sizing decisions by measuring the impact to transaction performance.

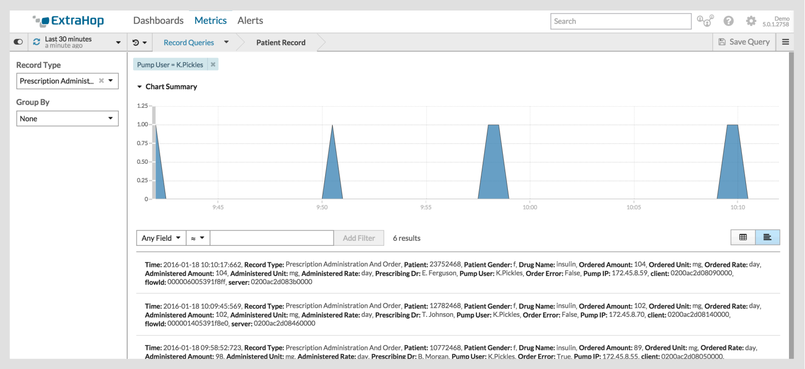
With ExtraHop, you get a seamless view of all your IT regardless of where it's running: in datacenters, remote offices, or the cloud. This comprehensive visibility makes security audits and compliance much easier. For example, InfoSec and IT Operations teams can see whether adequate encryption is used where it should be and whether insecure protocols are in use.

Gain Insights with Turnkey Analytics

Remote locations are often where business takes place. This is especially true in retail, field services, construction, oil and gas, hospitality, healthcare and transportation operations. Before the ExtraHop platform, there was no simple way to perform real-time analytics on what people are doing and how the business is performing. Frequently, each location would upload a batch report at the end of the night. Not only was the old way slow, but it was inflexible as well. With traditional Big Data methods, analysts would have to spend months integrating systems to consolidate the data or changing the system to meet new requirements.

The ExtraHop platform analyzes data in flight across distributed locations and enables anyone to perform analysis in real time. With this approach, you can gain deep insights into user activity and operational performance as it happens and without requiring data scientists. One nationwide retailer used ExtraHop to observe how the checkout process differed from store to store. They saw that their retail locations in Hawaii took much longer to complete the process and wanted to know why—it turned out that all the IT was working fine, but employees and customers on the islands were so friendly that they would simply talk together longer. These are the types of insights that often hide from organizations as they grow their operations and can have substantial impact on revenue.

The ExtraHop platform enables anyone to perform multidimensional analysis on transactions—without having to learn any query language.



Record Type: Prescription Administ...

Group By: None

Pump User = K.Pickles

Any Field ≈

6 results

Time: 2016-01-18 10:10:17:662, **Record Type:** Prescription Administration And Order, **Patient:** 23752468, **Patient Gender:** f, **Drug Name:** insulin, **Ordered Amount:** 104, **Ordered Unit:** mg, **Ordered Rate:** day, **Administered Amount:** 104, **Administered Unit:** mg, **Administered Rate:** day, **Prescribing Dr:** E. Ferguson, **Pump User:** K.Pickles, **Order Error:** False, **Pump IP:** 172.45.8.59, **client:** 0200ac2d08090000, **flowId:** 000006005391f8ff, **server:** 0200ac2d083b0000

Time: 2016-01-18 10:09:45:569, **Record Type:** Prescription Administration And Order, **Patient:** 12782468, **Patient Gender:** f, **Drug Name:** insulin, **Ordered Amount:** 102, **Ordered Unit:** mg, **Ordered Rate:** day, **Administered Amount:** 102, **Administered Unit:** mg, **Administered Rate:** day, **Prescribing Dr:** T. Johnson, **Pump User:** K.Pickles, **Order Error:** False, **Pump IP:** 172.45.8.70, **client:** 0200ac2d08140000, **flowId:** 000001405391f8e0, **server:** 0200ac2d08460000

Time: 2016-01-18 09:58:52:723, **Record Type:** Prescription Administration And Order, **Patient:** 10772468, **Patient Gender:** f, **Drug Name:** insulin, **Ordered Amount:** 89, **Ordered Unit:** mg, **Ordered Rate:** day, **Administered Amount:** 98, **Administered Unit:** mg, **Administered Rate:** day, **Prescribing Dr:** B. Morgan, **Pump User:** K.Pickles, **Order Error:** True, **Pump IP:** 172.45.8.55, **client:** 0200ac2d08050000,

Conclusion

Whereas IT organizations' traditional purview had been restricted to the corporate datacenter (and maybe a few branch offices), today's IT Operations teams are responsible for a diverse and sprawling portfolio of IT assets spanning datacenters, remote offices, SaaS providers, and public cloud environments. Unlike traditional monitoring tools, the ExtraHop platform provides real-time visibility into all these different environments, enabling IT teams to fix problems faster, optimize performance, protect against security threats, and derive business and operational insights.

Interested?

See how the ExtraHop platform works with our fully interactive online demo, which enables you to explore the user interface and walk through several scenarios: www.extrahop.com/demo

About ExtraHop

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop platform analyzes all L2-L7 communications, including full bidirectional transactional payloads. This provides the correlated, cross-tier visibility essential for today's complex and dynamic IT environments.

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

www.extrahop.com
info@extrahop.com
T 877-333-9872
F 206-274-6393

Customer Support support@extrahop.com
877-333-9872 (US)
+44 (0)845 5199150 (EMEA)