WHITE PAPER

ExtraHop

Enhance Your Application Performance Management Strategy with Wire Data

Utilize the ExtraHop platform to champion end user experiences, hold vendors accountable, and demonstrate IT Operations' value to the enterprise

Ensuring Commercial Application Performance Starts with Regaining Lost Visibility

Many businesses rely on on-premises commercial software applications, such as SAP enterprise resource planning software, Epic Systems electronic healthcare records systems, and Manhattan Associates supply chain software. Yet newer agent-based application performance monitoring approaches can't be deployed on these applications, either due to risk of voiding service agreements or because the applications aren't written in supported languages—leaving IT Operations teams without sufficient visibility to resolve some performance issues.

This whitepaper explores the benefits of leveraging untapped wire data in your network, how the ExtraHop platform correlates this data to provide greater visibility into application performance, and how IT Operations can use ExtraHop to expedite data visualization, analysis, and issue resolution for higher application performance.

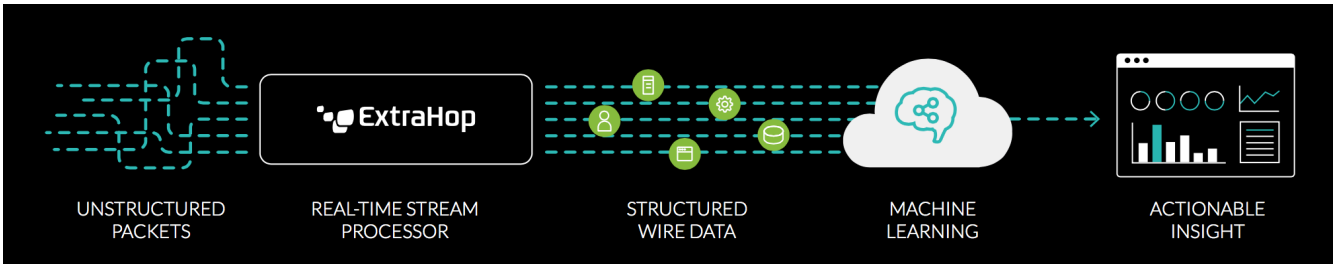
In APM, What You Can't See Can Hurt You

From healthcare records to retail inventory management, manufacturing processes to oil and gas exploration, many enterprises rely on commercial software applications—such as SAP enterprise resource planning (ERP), Epic medical records systems, and Manhattan Associates supply chain and warehouse management software. These applications are ingrained in key processes, yet many enterprises have little recourse for gaining visibility into these applications' performance besides calling the vendor and hoping for the best.

Agent-based application performance management (APM) products can't be deployed on applications without voiding service level agreements (SLAs), or simply because the applications are not written in supported languages. For understaffed IT Ops teams already facing reactive "firefighting" scenarios, this lack of visibility makes it difficult to determine if application performance issues are in their network or server infrastructure or stemming from the software itself.

Gain Application Performance Insight with Wire Data

Deployed passively without agents, the ExtraHop platform uses real-time stream processing to transform network communications into structured wire data at line rate. Upon receiving a copy of network traffic from a tap or port mirror, the stream processor performs decryption, full-stream reassembly, and protocol decoding for every transaction to extract both network and application-level details such as errors, methods, file names, and users.



Key features and differentiators of the ExtraHop platform include:

- **Line-rate SSL decryption:** If the traffic is encrypted, the platform performs bulk SSL decryption at up to a sustained 40 Gbps with native hardware acceleration. This level of scalability is unique to the ExtraHop platform, and enables IT Ops to discover, observe, and analyze every digital interaction as it happens at a fraction of the cost per Gbps of analysis compared to other real-time analytics platforms.
- **Full-stream reassembly and wire-protocol decoding:** The real-time stream processor recreates the TCP state machines for every sender and receiver communicating on the network. This allows the processor to reconstruct complete flows, sessions, and transactions and is a prerequisite for deeper application-protocol analysis.
- **Application-level content analysis:** After reassembling packets into full streams, the stream processor analyzes the payload and content from Layer 2–7, auto-discovering and classifying any device or client communicating on the network. The platform also continuously maps the relationships between all clients, applications, and infrastructure communicating on the network. More than 4,000 metrics are measured and recorded out-of-the-box and associated with these auto-discovered systems.

Use Your New Insight to Hold Software Vendors Accountable

When it comes to troubleshooting application performance issues, software vendors have historically enjoyed the benefit of the doubt. In cases where an enterprise's end users experienced performance issues with a commercial application, IT Operations teams might report the issues to their vendor. Assuming the enterprise hadn't voided the vendor's support agreement, the vendor could opt to help troubleshoot—but could also redirect the onus on the enterprise, citing the need for more server hardware or blaming network congestion.

With ExtraHop, customers hold more sway in the vendor-customer relationship because they can see the factors attributable to application issues. If a particular database SQL method is taking an unusual amount of time, IT Operations can see it. If network transfer and server processing is taking too long, they can see it. If only a subset of clients is experiencing slowness, they can see it. What's more, ExtraHop makes forensic evidence available for IT Operations to prove its innocence.

ARBITRATION THROUGH WIRE DATA

The IT Operations team at Middlesex Hospital uses reports from ExtraHop to show internal and external application teams how their applications are behaving in the production environment. Reports can be generated from ExtraHop at the push of a button. The example above shows the database query SELECT * FROM PRODUCT has been run 80,018 times over a 30-minute period, indicating a mistaken application code change. This type of insight is invaluable when discussing application performance with application teams.

For instance, it's not uncommon for hospitals and other healthcare organizations to spend millions of dollars annually on Epic electronic health record (EHR) systems. Not only is this application typically complex to manage, but Epic also requires its customers to maintain a performant hardware infrastructure. Not doing so can result in financial penalties. ExtraHop has been used by dozens of healthcare organizations to ensure that their on-premises infrastructure running Epic is efficient and compliant. In turn, these enterprises can prove their SLA is being met and get the best licensing discounts with Epic, while also having evidence in their back pocket to hold Epic accountable if performance issues arise.

Use Case: ERP Application at a Large Media Company

A film and television production/distribution company was running SAP across multiple locations. The company was experiencing ongoing performance delays in its SAP environment, and as more users were affected, more blamed the network.

Using ExtraHop, the company's IT Operations team was able to auto-discover and auto-classify various SAP components (i.e., different functionalities that can be purchased and added by clients) based on hostname prefixes in network transactions. Comprehensive performance dashboards provided deep visibility into web, DNS, database, and storage traffic for each component environment.

IT Operations was quickly able to pinpoint tens of thousands of Nagle Delays per day in their SAP environment, indicating a misconfiguration of the TCP profile on the application server. In-house SAP engineers were able to take this evidence to SAP itself, where SAP's support engineers pointed them to a relevant solution associated with enabling the Nagle's algorithm on the server—contrary to what was recommended in the vendor documentation.

Complement Existing APM Investments for a Holistic Perspective

By providing objective and actionable wire data, ExtraHop complements the application and log monitoring solutions you may already use.

COMPARING DATA SOURCES USED FOR APPLICATION PERFORMANCE MONITORING	
Wire Data	• Extracted from the network traffic • Includes application-level details such as errors, methods, and users • Represents a tremendously rich source of IT and business intelligence
Machine Data	• Ubiquitous time-series, event-driven data • Self-reported information about device performance and activity • Can help IT teams identify overburdened machines, plan capacity, and perform forensic analysis of past events
Agent Data	• Derived from bytecode instrumentation and call stack sampling • Useful for specific applications or devices that require code-level monitoring • Vital to DevOps

The following use cases detail the benefits of using ExtraHop's and complementary traditional APM solutions, such as AppDynamics, NewRelic, or Splunk:

- A joint customer in Southern California wanted L2-L4 metrics (network delivery) from ExtraHop to be streamed into their traditional APM solution via the custom metrics API. This enabled them to incorporate network delivery metrics into their existing APM solution's dashboards for database, memcache, web, and storage.
- A bank in Canada uses a traditional APM solution to instrument multiple applications, but could not instrument their SAP application without violating the support agreement. The APM vendor asked for ExtraHop's help in extracting front-end user metrics from wire data and then representing those in their dashboards. The dashboards include click-through links to ExtraHop for further exploration.
- A regional bank in the United States uses ExtraHop to monitor the performance of the majority of their applications, but uses a traditional APM solution to get detailed instrumentation of a subset of more critical applications.

Customer Success: Middlesex Hospital

Challenge: Middlesex Hospital manages a diverse and ever-expanding array of applications and services, including Cerner, eClinicalWorks, and McKesson Homecare. Troubleshooting was time-consuming for the IT team, and even when the team could successfully identify a problem, their monitoring tools didn't always provide the clear evidence needed to convince vendors and internal app teams.

Solution: The Middlesex IT team had primarily used packet-capture tools for troubleshooting and forensic analysis, and investigated ExtraHop to get real-time insight into all L2-L7 communications between systems. ExtraHop offered:

- Objective data for IT troubleshooting
- Pinpoint precision in real time

Results: The Middlesex IT team has been able to dramatically reduce the time spent troubleshooting complex problems with ExtraHop while also expanding and sharing insights across the organization.

- 90% faster MTTR for complex problems
- Better accountability from third-party vendors
- Precise insight into performance issues

CUSTOMER BACKGROUND

Connecticut-based Middlesex has been ranked one of the Top 100 Hospitals in the U.S. by Reuters, with a 200-bed community hospital and over 30 offsite facilities.

Industry	Healthcare
Commercial Applications	Cerner, eClinicalWorks, McKesson Homecare

> "Before, when we would send a packet capture back to the vendor, they might not understand what they were seeing. With ExtraHop, it's the difference between the vendor believing us and the vendor not believing us—or the difference between getting to the root cause of a problem now versus getting to the root cause of a problem weeks from now, after exhausting every other possible avenue."
>
> **Ant Lefebvre**
> **Sr. Systems Engineer**
> **Middlesex Hospital**

Gain Full Visibility into Application Performance with ExtraHop

Today, the network is the lifeblood of every digital business. Knowing what's happening in the network in real time not only empowers IT Operations to address issues faster and hold vendors accountable for performance issues, but it also helps change the organization's perception of IT Operations from reactive scapegoat to a strategic revenue-supporting asset. Leveraging ExtraHop as part of your APM strategy can help your IT Operations team attain these outcomes and better support the business.

To learn more, try out the ExtraHop demo online at www.extrahop.com/demo.

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)