WHITE PAPER

ExtraHop

Delivering Visibility for Your Risk Management Framework

Abstract

For organizations that have prioritized the Risk Management Framework, there still remains much work to be done, particularly when it comes to optimizing visibility for systems governed by this Framework. Without broad and deep visibility, the output of this model can be glaringly inaccurate, especially considering that the greatest challenges for security experts aren't the known issues but rather the unknown issues that have not yet even been discovered.

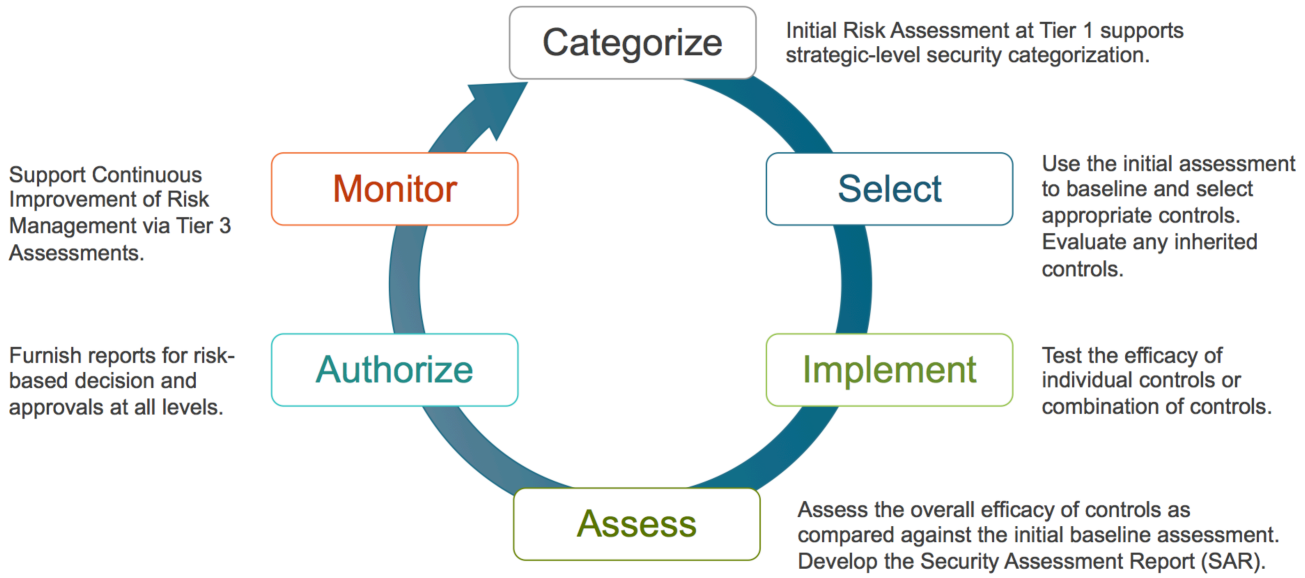
This paper will explain how real-time wire data visibility can shorten the feedback loop of a Risk Management Framework, greatly increasing its responsiveness and effectiveness, and provides the strongest and most accurate posture when addressing risk: an unbiased, real-time view into what is actually happening on a network.

This real-time visibility supports five Risk Management Framework steps: Categorize, Select, Implement, Assess, and Monitor.

Using Wire Data to Support the Risk Management Framework

Your network is a rich source of real-time data but mining that data in flight at scale has never been possible until now. The ExtraHop platform makes sense of your data in flight so that civilian, defense, and intelligence agencies can effectively use this rich wire data to assist with:

1. Baselining, Characterizing, and Documenting existing or new systems in output formats such as Visio, PDF, or Excel.
2. Developing a comprehensive Security Assessment Plan by using wire data analytics and reports.
3. Risk Assessments during various stages of the RMF process, leveraging a common data source that produces output formats specifically tailored for different stakeholders.
4. Risk assessment documentation (diagrams, data sets, KPI reports). Corresponding wire data metrics can be used in conjunction with a Central Repository for Authorization Documentation (i.e. Body of Evidence [BOE]) to produce the Security Assessment Report (SAR) and other activities such as an Operational Authorization to Test (OATT), Authorization to Proceed (ATP), and Authorization to Operate (ATO).
5. Arming multiple levels of stakeholders with a definitive source of information to aide in the development of risk mitigation strategies, solutions and recommendations.
6. Other Assessment activities such as "Red/Blue Team" activities can be supported with wire data metrics and documentation.



Real-time visibility into wire data supports five of the Risk Management Framework functions, including assessments for Categorize, Select, Implement, Assess, and Monitor.

With the ability to explore and report against wire data in a number of different ways, teams can support Risk Management Framework (RMF) functions above and beyond risk assessments as described in the sections below.

Step 1: Categorize

Real-time stream processing of network traffic to produce wire data will enable organizations to determine the appropriate security category of a system by auto-discovering and classifying all component devices, and mapping ports, protocols, and services (PPS)

together with corresponding transaction-level details. This zero knowledge approach conclusively determines what devices, services, and data comprises a system, as well as helps defines the security level and boundary of a system based on detected device interactions and dependencies. Device attributes such as IP and MAC addresses, along with PPS and relevant Layer 7 transaction information such as username, database query, application request/reply details, files, and many others, are captured and transformed into wire data that can be visualized, explored, reported on, or shipped off to an external platform. A robust wire data analytics platform will support a broad range of industry standard protocols as well as the ability to add new custom protocols as needed.

After baselining an "as-is" or "to-be" information system, the collected wire data metrics are used to support decisions for the selection of mitigating controls in step 2 of the RMF process. These metrics are rich and encompass a wide spectrum of attributes within the network and application layers of the Open Systems Interconnect (OSI) stack and can provide valuable insights into what's transacting within your environment.

Real-time wire data analysis provides organizations with a comprehensive view of all activity in their environment.

Step 2: Select

Wire data analytics supports two aspects of the Select step: 1) The use of a third-party to provide observed artifacts gathered during the Categorize step to support the selection of appropriate security controls to reduce the identified attack surface and, 2) Providing an objective continuous monitoring solution for all data-in-transit for the system under evaluation. Selecting controls based on the results of real-time wire data analytics yields far more accurate results than relying on sporadic system assessments, synthetic transactions, or outdated documentation.

Step 3 and 4: Implement and Assess

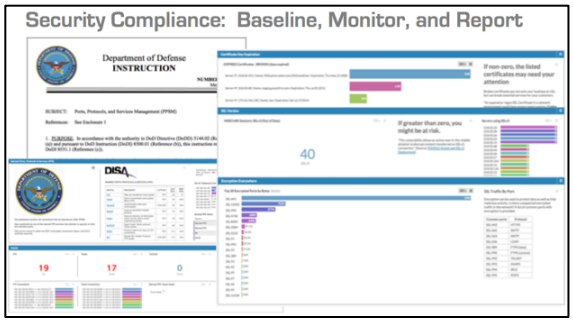
By analyzing all services and transactions in real-time, and comparing specific wire data metrics against what was observed during the Categorize and baseline stage, the wire data analytics platform can reveal whether the selected controls are functioning appropriately within the context of live information system traffic, a stronger posture than merely confirming that controls were

implemented by configuration review or point-in-time synthetic transactions. With a passively obtained set of metrics you can effectively measure and report against the efficacy of these controls.

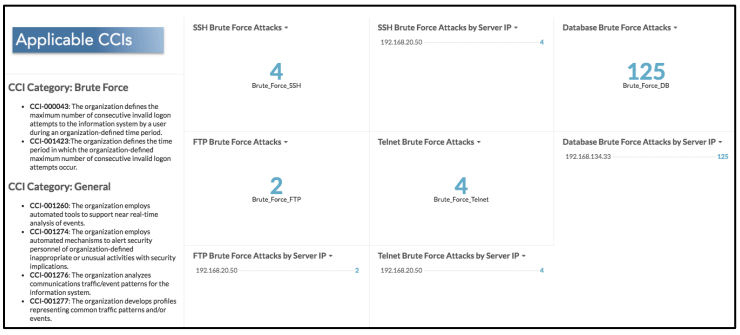
Step 6: Monitor

Wire data analytics enables constant and complete observation of your environment at the highest level to easily identify anomalous and disruptive behavior from any device or user. Through the passive observation of data-in-motion, the wire data analytics platform provides a trusted source of information because data-in-motion is not self-reported the way log files and other data-at-rest information sources are. Many of the Control Correlation Identifiers (CCIs) specified by the NIST RMF standard are readily monitored by this real-time analysis of data in motion, and fall into a number of categories, including:

- General network traffic continous monitoring
- Brute force detection
- Cryptography audit
- Device inventory
- Data exfiltration
- Ports, protocols, and services
- Remote access monitoring
- Covert channel monitoring
- User monitoring



Monitoring banned PPS in support of the DISA PPSM standard

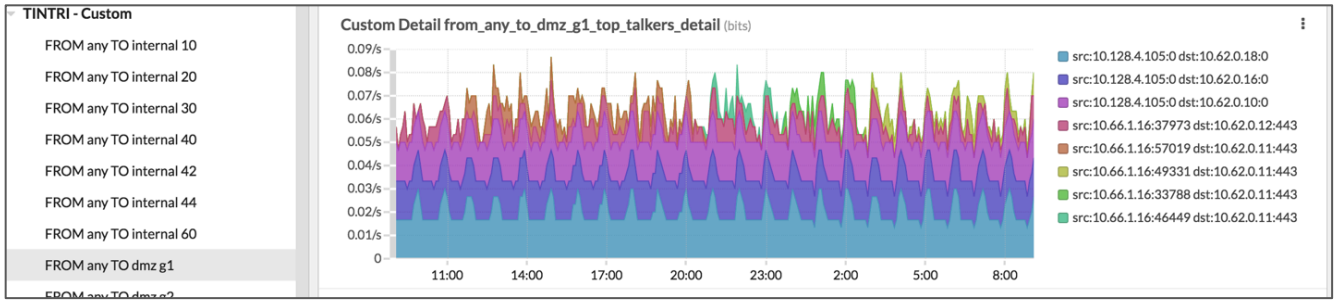


Monitoring brute force attacks against multiple services

Continuous Monitoring Example

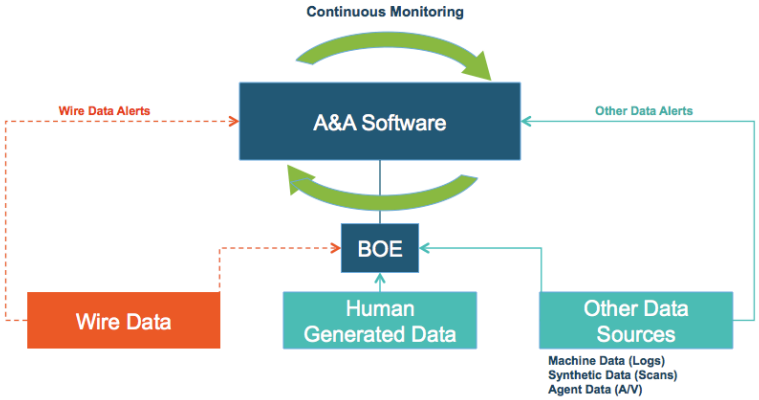
Wire data analytics can be used to continuously monitor all aspects of transactions seen on the network in support of RMF Step 6: Monitor. For example, in a "zero trust" environment, ExtraHop continuously audits thousands of metrics for both allowed and disallowed transactions, and provides an easy way to produce the relevant reports in the BOE that support what was authorized to transact.

As an example, the table below shows what was allowed, or not allowed, between specific zones, network segments, or enclaves. These could align with authorization boundaries or segments within the same boundary. This table could serve as the BOE artifact that notates what was approved to transact on the network, with definitive metrics coming from all observed transactions.



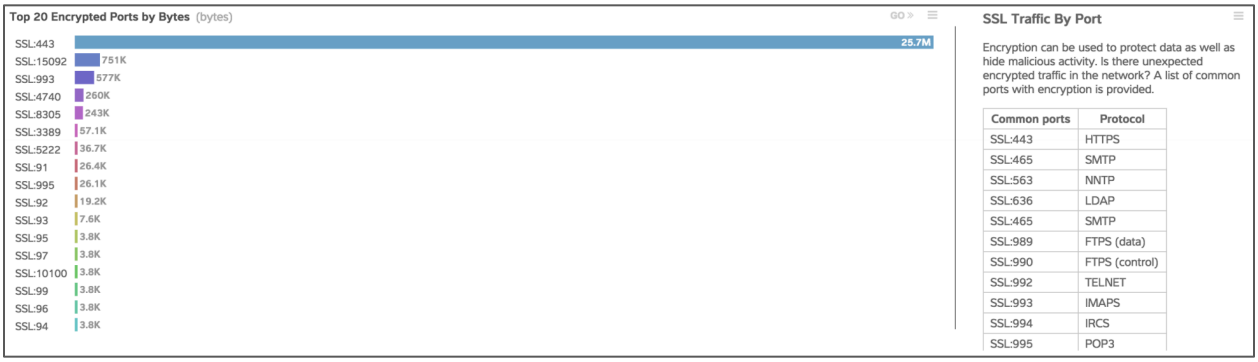
Continuous Real-Time Monitoring Dashboard using ExtraHop

For increased monitoring, wire data metrics can be sent to third-party tools to enrich their data by adding insights into all network and application transactions. This is achieved with a rich set of open-standard APIs, allowing for both PUSH and PULL capabilities. Wire data can be streamed continuously, or selectively when certain conditions arise either through the manual configuration of thresholds or using ExtraHop's built-in trending and alerting functions. Automation and Orchestration can be achieved by integrating ExtraHop with other tools that also support open-standard APIs such as REST, SNMP, and SMTP.

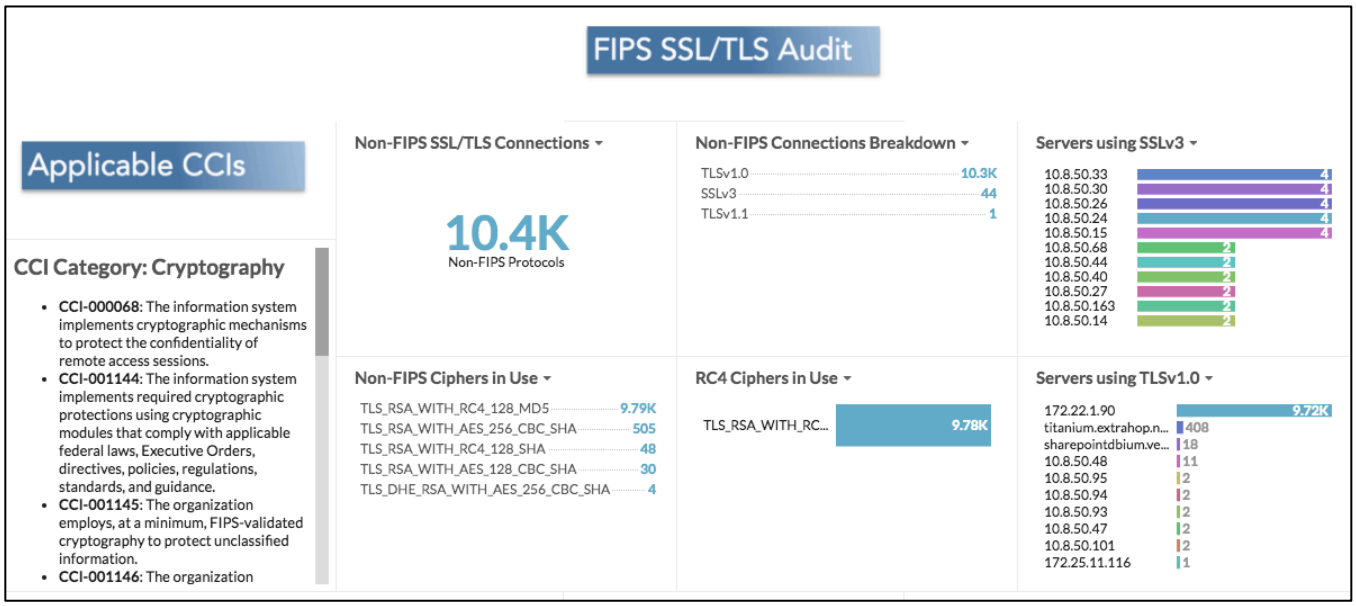


In further support of RMF continuous monitoring activities, ExtraHop can send wire data artifacts to an RMF BOE and Authorization and Assessment software tool. Examples of what could be monitored, in real-time, and reported with through the use of wire data include:

- SSL Certificates – Check the validity of certs and find any expired certs. Are they self-signed?
- Encryption – Are connections compliant with Federal data-in-motion encryption requirements? What cipher suites and SSL/TLS versions are being used and which hosts and applications are using non-FIPS compliant ciphers/protocols?
- Unusual DNS Requests – Why is that workstation making 19,000 DNS requests a minute, and why are most of them TXT records? Why are there 14 DNS servers in your environment when there should only be 4? Is DNS tunneling occurring?
- Map and Diagram Network, Host and Application Relationships/Data Flow – Which devices are communicating with each other? Using what protocols and how often? How much data is transferred, and in which direction?
- New Device Reports and Actions – Alert when a new device shows up on the network and use an ExtraHop API call to trigger a command on a NAC system which can scan, interrogate, or block the new device.
- All IP addresses transacting on the network – Visibility of devices should not be dependent on their ability to be configured to support logging or SNMP. All devices which transact on the network should be immediately discovered.
- Application Resources – Databases, Application Resource Artifacts, File Shares and who is accessing these resources (Admin, Service, or other accounts)
- Monitoring VPN and VDI/Citrix access and profiling users and the applications they use



Real-time encrypted traffic monitoring and reporting



Real-time audit of SSL/TLS server transactions using non-FIPS compliant ciphers and protocols

SDLC and DevOps Association with RMF

Wire data analytics can be leveraged across IT organizations, even outside the realm of security. In a DevOps scenario, the wire data analytics platform can monitor staging and production environments and provide real-time and historical context around changes to applications, security parameters, and even network components. Wire data empowers application, networking, and engineering teams to easily monitor and measure security and performance across all stages of an application's lifecycle. Wire data promotes collaboration and breaks down silos, allowing teams to quickly determine whether a performance problem was due to infrastructure, misconfiguration, a rolled-out security patch, or even a code issue. Real-time analysis of all transactions provides the data that cross-functional AGILE teams can rely on where incremental, iterative work cadences between teams and systems happen at a rapid pace.

With non-invasive monitoring for wire data in the staging environment, engineering teams can observe the behavioral impact of new code against baselined performance and continuously tune for performance and security. Operations teams will be able to accelerate

application updates and rollouts because they know the expected behavior before a release and have full dependency understanding during and after the release, dramatically reducing risk.

Wire data can be utilized during many System Development Lifecycle activities. For example, when assets are scheduled for decommissioning, Organizations can objectively validate that the hardware and software tied to those assets are indeed gone. By examining and reporting against any remaining activity tied to those assets, stakeholders can be assured that the assets are no longer participating on the network.

RMF steps and the association back to the software development lifecycle (SDLC)

Cloud Migration Monitoring

Architectures and systems change constantly. Transformational endeavors take shape such as cloud migration, data center consolidation, or disaster recovery and planning. Wire data provides a means to baseline, measure, test, assess, and report on the activities surrounding these initiatives. For example,, a dashboard can be created to uses wire data to provide insights to engineering, operations, and management teams on application performance in the "cloud" as it relates to the legacy data center. Both front- and back-end transactions would be monitored to include all application dependencies. Security posture can be assessed using these same techniques to ensure that no data is "leaking" outside of the cloud and that no other hosts are connecting to the services when they should not be (e.g. external IP addresses).

Wire Data Analytics for Red/Blue Teams

Real-time analysis of all transactions on the network (data-in-motion) allows hunt-and-protect teams the ability to identify, observe, and measure behavior seen on the network. This constant and complete observation of your environment enables Red/Blue Teams to easily identify hosts, services, transactions, and anomalous/disruptive behavior from any device or user, or perform reconnaissance for vulnerability/penetration testing. Wire data serves as a trusted source of information because data-in-motion is not self-reported the way log files and other sources are. With wire data analytics, Red/Blue Teams can:

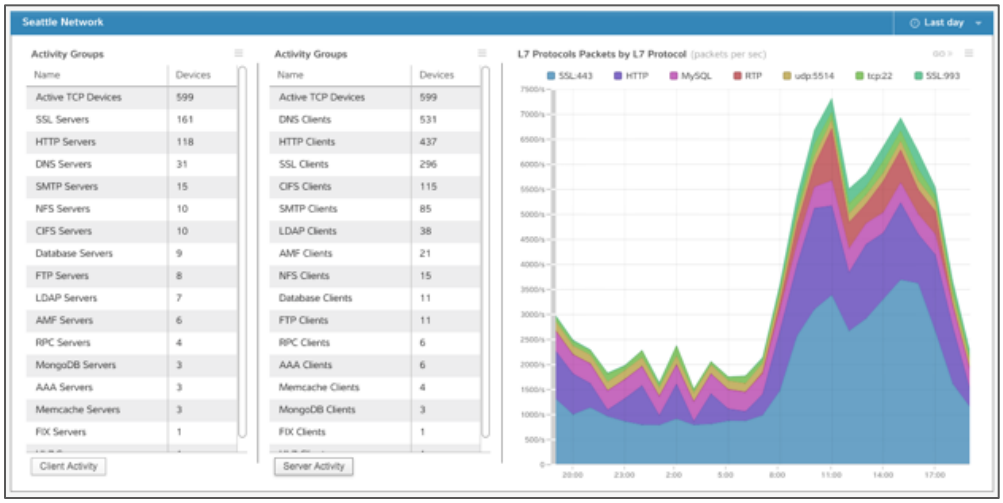
- Identify and investigate anomalies and determine the root cause of events
- Effectively perform interactive, active threat hunting with a comprehensive and intuitive workflow, allowing visibility into all

devices and protocols on a network without a high learning curve.

- Monitor use of banned ports, protocols, and services
- Enumerate services for penetration/vulnerability testing
- Automatically discover and map dependencies for devices communicating on the network
- Support large and dynamic environments with real-time analysis up to 40 Gbps sustained throughput on a single appliance.

Wire data analytics can be used for indexing, trending, and delivering predictive alerts. As metrics are indexed, the analytics platform classifies newly discovered devices based on heuristic analysis of machine information and behavior. For example, if a device responds to database requests, then it is a classified as a database server. If it is also responding to DNS requests, the device is also classified as a DNS server.

The platform automatically builds activity baselines for all clients, systems, applications, and infrastructure so that you can receive predictive trend-based alerts when something is out of the ordinary. You can also customize alerts based on behaviors like anomalous network activity, web application and database errors, unusual payload size, slow transactions, poor end-user experience, and expiring SSL certificates.



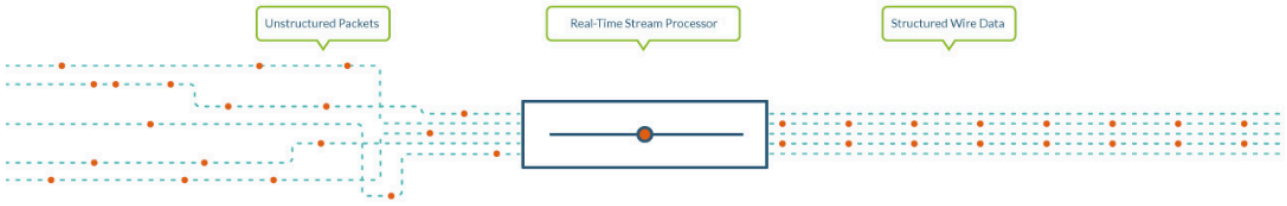
Detect devices and applications traversing the network.

About ExtraHop Networks

ExtraHop Networks, Inc. is an enterprise technology and analytics company headquartered in Seattle, Washington and is the global leader in real-time wire data analytics. ExtraHop has been in business since 2007, and began shipping products to customers in 2009. ExtraHop has been selling into Federal Agencies since 2011 and has production units supporting a number of Federal Civilian, DoD, and Intelligence Agencies. All engineering and support for the ExtraHop platform resides within the United States, and ExtraHop has dedicated Federal sales and product management teams located within the Washington D.C. Metropolitan Area.

ExtraHop Platform

The ExtraHop platform is a simple turnkey solution that empowers you to make sense of all data passing over the network. All technologies and applications transact and communicate on the wire, and if you want to gain visibility and control risk, it all starts there—by analyzing your data in real-time while it is in motion.



Wire data comprises L2 – L7 data spanning the entire application delivery chain. Through real-time full-stream processing, unstructured data is reassembled into structured wire data that can be analyzed in real time and mined for insights

Data passing over your network is data in motion, as opposed to data at rest, which is stored for offline analysis. Your data in motion is the most valuable source of information that your organization can mine for insights. But to access your data in motion, you need a platform for transforming large volumes of unstructured network packets into structured wire data. The ExtraHop platform is built to do exactly that at an unprecedented scale.

It is important to understand that the ExtraHop platform is a completely passive out-of-band solution, requiring no agents, no host configurations, and no credentialed access. It will provide maximum visibility into the transactions occurring within your network with no degradation or disruption to the existing systems, applications, or users. It will not actively interrogate any devices, nor will it add any additional traffic to the networks that it is monitoring. ExtraHop is agnostic in this sense, and being fluent in industry standard protocols such as TCP/IP, it can monitor activity involving any devices using these protocols, such as mobile devices, Internet of Things, and legacy devices and systems.

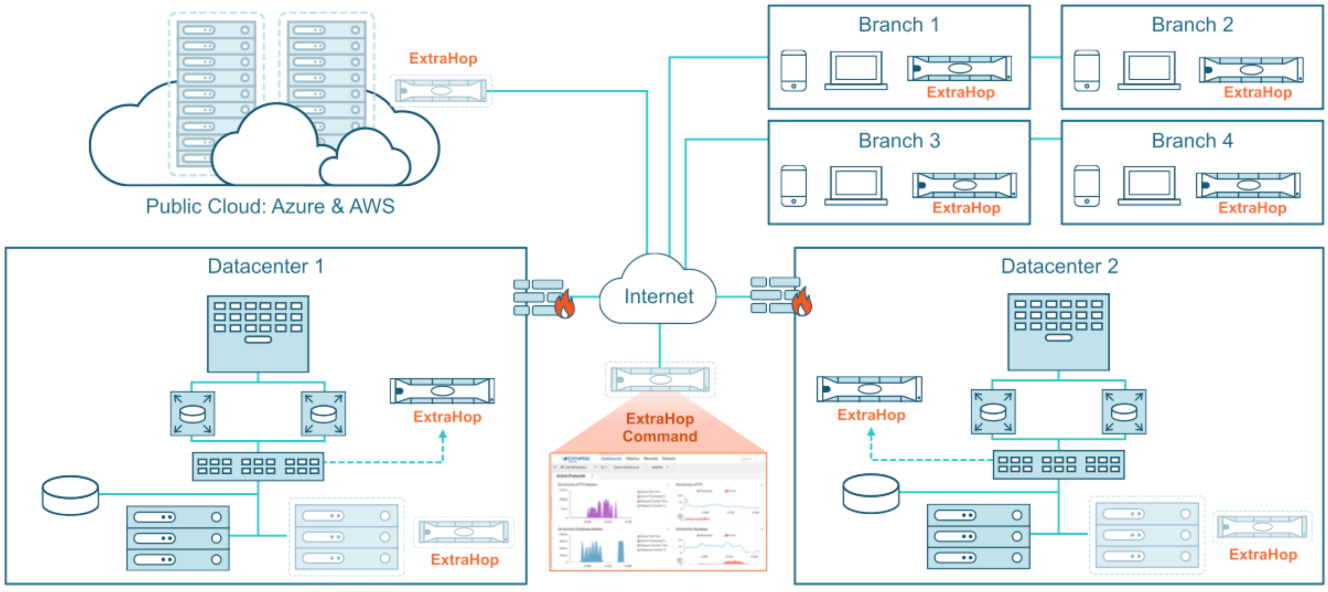
Enterprise-Wide Visibility

As an information security professional, you can't tolerate reduced insight due to increased scale, dynamism, and complexity in your environment. Limited visibility results in a loss of compliance control, inability to assess and report, but even more importantly, data breaches and frustrated analysts.

The ExtraHop platform can be deployed across a large geographically dispersed enterprise for a holistic view of all wire transactions throughout the network. The approach is simple and scalable, and provides users of the platform a single pane of glass view into all wire data collected across the enterprise. Regardless of whether the network to be analyzed is physical or virtual, private or public (Cloud), ExtraHop can be easily and seamlessly deployed across a heterogeneous environment. Connectivity between ExtraHop

appliances is achieved via lightweight communications secured with SSL (TLS 1.2), making the platform ideal for enterprises with limited-bandwidth remote sites.

For additional information regarding ExtraHop's support for an enterprise-wide monitoring solution please see the white paper *IT Visibility Across Datacenters, Remote Locations, and the Cloud*: https://assets.extrahop.com/whitepapers/ExtraHop-Across-Datacenters-Remote-Locations-and-Cloud.pdf



The ExtraHop platform supports the entire environment across datacenters, remote offices, and the cloud.

ExtraHop Family			
ExtraHop Discover Appliance Provides a global view of the environment. Feed it network traffic from a tap or port mirror, and it transforms packets into structured wire data for highly scalable real-time IT and business analysis.	**ExtraHop Explore Appliance** Receives transactions and flow records from the Discover appliance and indexes them for quick multidimensional analysis. Allows you to search and explore every interaction via an intuitive visual user interface.	**ExtraHop Trace Appliance** Traces activity back to the source. Provides the ability to filter down to just the packets you want to analyze tied to specific events, delivering a simplified rapid workflow from top down or bottom up.	**ExtraHop Command Appliance** Take command of your data streams from Discover appliances across datacenters, the cloud, and branch offices. Merges data to create a centralized view and the ability to manage all your data in one place.

Conclusion

By adding wire data to your Risk Management Systems and integrating a real-time visibility approach to your RMF you can improve control in even the most dynamic environment. When developing your monitoring strategy, it is important to consider:

- How easy is it to collect data and make sense of it?
- The breadth and depth of visibility each solution offers.
- The impact monitoring can have on the environment itself.
- How susceptible is your system to be altered by malicious actors?
- Can the information be obtained and acted on rapidly?

The ExtraHop platform is purpose-built to address all of these considerations, and greatly strengthens the security posture and level of visibility within a Risk Management Framework.

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

www.ExtraHop.com
info@ExtraHop.com