



The ExtraHop Platform for Defense Agencies

ANALYZE DATA-IN-FLIGHT FOR SITUATIONAL AWARENESS

“The ExtraHop platform enables our DoD clients to gain new perspectives on their environments. This is our looking glass into the cyber domain, from baselining the as-is environment to delivering complete situational awareness on performance and security across the hybrid cloud.”

— **Kurt L. Hodges**
Retired DoD Official

BENEFITS

- Equip cyber hunter and protection teams to identify and investigate anomalies
- Monitor use of banned ports, protocols, and services
- Automatically discover and map dependencies for devices communicating on the network
- Improve delivery of virtual desktops and apps (e.g. Citrix) with end-to-end visibility
- Support large and dynamic environments with real-time analysis up to 40 Gbps

Your network is your richest source of real-time data to meet mission goals and save lives, but mining that data in flight for situational awareness has never been possible until now. The ExtraHop platform makes sense of your data in flight so that defense agencies can more effectively ensure mission success. With the ability to explore their wire data, teams can remediate issues faster, optimize performance, secure systems, and plan for consolidation and migration initiatives.

DISCOVER EVERYTHING IN YOUR ENVIRONMENT

Everything transacts on the wire. ExtraHop analyzes this data in flight so that you can see every device and application in real time. The platform’s automatic discovery and classification capabilities restore control to agency personnel that manage large, dynamic, and heterogeneous environments.

- Identify security weaknesses and attacks
- Easily track IT assets and map dependencies
- Gain visibility in dynamic virtualized environments
- Deploy simply, without agents

GAIN UNMATCHED VISIBILITY

ExtraHop delivers actionable insight to your mission teams so that they can isolate and diagnose hidden problems in your environment. Wire data is also a trusted, empirical source of information—you know something happened because you observed it on the wire.

- Drill down to see transaction details for specific users and devices
- Monitor all outbound connections from your critical servers
- Correlate activity across technology tiers
- Equip all teams with a shared, trusted source of data
- Define and implement custom metrics in minutes

EXPLORE YOUR WIRE DATA WITH TURNKEY ANALYTICS

With ExtraHop, your teams can easily explore their wire data to find real-time issues and investigate historical activity.

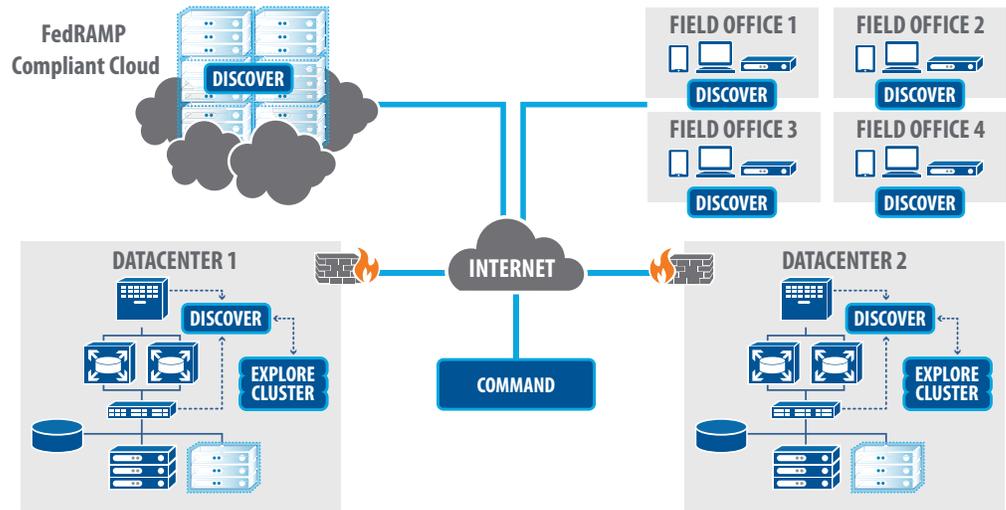
- Rapidly respond to security incidents and perform forensic investigations
- Enable everyone to use Big Data analytics—no data scientists required
- Ensure compliance with security and privacy regulations
- Stream wire data metrics to other platforms, such as Elastic, Splunk, LogRhythm, Arcsight, and AppDynamics

EXTRAHOP DISCOVER APPLIANCES

	Throughput	Servers Monitored
PHYSICAL	Up to 40 Gbps	Up to 5,500
VIRTUAL	Up to 10 Gbps	Up to 3,000
CLOUD	Up to 10 Gbps	Up to 3,000

EXTRAHOP EXPLORE APPLIANCES

	Records per second (data ingestion rate, single node)	Storage and lookback
PHYSICAL	Up to 35,000	11 TB onboard
VIRTUAL	Up to 35,000 (full resources)	Up to 4 TB per node



The ExtraHop Discover appliance is the linchpin of the ExtraHop platform. 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.

The ExtraHop Explore appliance receives transaction and flow records from the Discover appliance and indexes them for multidimensional analysis. You can search, explore, pivot, and extract insight from it at any time.

The ExtraHop Command appliance merges all your data streams from Discover appliances across datacenters, the cloud, and branch offices. You can centrally view and manage all your data in one place.

THE BOTTOM LINE FOR DEFENSE AGENCIES

The ExtraHop platform is a force-multiplier for DoD cyber hunt, protect, and IT teams. The platform enables defense agencies to mine their richest source of data—the data in flight on their network—for real-time, actionable insights.

ExtraHop enables cyber and IT teams to discover, observe, and analyze everything in their IT environments. As long as it communicates on the network, the ExtraHop platform will detect and classify it. As an example, agencies can monitor all outbound connections and detect any banned ports, protocols, and services on their network. Personnel can also dig deep into details, exploring details for web, database, authentication, storage transactions, and more. With ExtraHop wire data analytics, we sift through the noise allowing you to get from data to decisions much quicker.

ABOUT EXTRAHOP NETWORKS

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

877-333-9872 (voice)

206-274-6393 (fax)

info@extrahop.com

www.extrahop.com



Passively discover and explore devices, ports, protocols, and services (PPS).