ExtraHop for Security and Compliance

Your Network Is Already a Security Platform

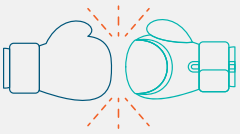
With the ExtraHop platform, you can tap into the richest and most real-time source of security visibility: your network. ExtraHop provides you with full visibility into all behavior on the network so that you can detect threats faster, identify weaknesses in your environment, and make your security tools smarter.

At-a-glance

- North-south, east-west visibility
- Real-time insights
- Deep analytics with long lookback
- Streaming to SIEMs

"ExtraHop shows what the applications are actually saying, not just who is talking to whom."

— Micah Rodgers, Senior Network Security Engineer, Murphy USA



Wire Data vs. Log Data

As security organizations build up their analytics capabilities, they should evaluate which data sources to rely on. Wire data offers a richer and cleaner dataset than logs, with broader coverage. By adding wire data to your analytics strategy, you can increase the signal-to-noise ratio of your SIEM or other analytics platform.

Learn more by downloading the whitepaper:

How to Get More Signal, Less Noise for Your SIEM

You don't know what the next threat will be, but one thing is certain: It will involve two machines communicating over the network. With ExtraHop, you can rethink your network as a source of security visibility—constantly flowing data about what's happening across your IT environment.

See What's Hiding

Detect threats faster inside your environment

Every attacker relies on the network, which leaves them nowhere to hide when you have the ExtraHop platform deployed. Because ExtraHop looks at network traffic, this means you can spot risks even on systems where you don't have an endpoint agent installed or logging instrumented.

Strengthen Your Defenses

Mitigate high-priority risks

Strengthen defenses by identifying and mitigating high-priority risks. ExtraHop provides continuous auditing of your environment so that you can spot weak cipher suites, banned protocols, and more.

Make Your Tools Smarter

Stream wire data to your SIEM platform or next-gen firewalls

You can enrich your existing security toolset by streaming real-time events and metrics from ExtraHop into other platforms. This adds a valuable new dimension for incident responders and can trigger smart automated responses, such as network access control actions.

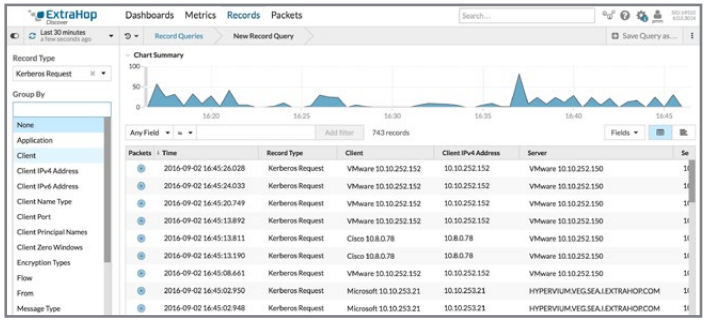
ExtraHop's Geomaps function can track real-time user activity by location to identify potential threats. The screenshot above shows DNS queries to IP addresses in Russia.

Example Use Cases

The ExtraHop platform provides full visibility into the network, the common denominator for any threat. Our enterprise customers rely on ExtraHop for dozens of security use cases, many of which could not be feasibly addressed with other products. The ExtraHop Solution Bundles Gallery contains packaged customizations for many of the use cases below.

Active Directory Monitoring	Track authentication failures, superuser account activity, and other login statistics. ExtraHop also records access failures and other metrics for other AAA services, including Kerberos, Radius, and Diameter.
CVE Detection	Detect network activity associated with vulnerabilities, such as Heartbleed, Freak SSL, and POODLE.
Database Activity Monitoring	Identify suspicious database activity, such as DROP and DELETE methods, and large database requests.
Device Discovery	Discover and classifies new devices on the network during specific periods.
DNS Monitoring	Uncover DNS tunneling, fast flux, exfiltration activity, and external queries to suspicious geographies. ExtraHop provides high-level dashboards for this activity as well as the ability to explore DNS transaction records.
Ransomware Mitigation	Detect CIFS activity associated with ransomware, automate NAC and firewall actions, and recover files with precision packet capture.
SSL Auditing	Track SSL versions in use and cipher suite strength for every session in your environment.
Scan Detection	Detect malicious network and port scans, including ARP and ICMP for host scans, and various other TCP and UDP scans.

Identify risks with customizable dashboards that provide a high-level view of activity in your environment.



Speed investigations by exploring transaction records, with the ability to download the associated packets.

Try the Online Demo!

See what the ExtraHop platform can do for security use cases in our online demo. You can explore the interface for yourself or follow guided tours, including for ransomware detection and threat detection.

www.extrahop.com/demo