ExtraHop for Security and Compliance

IF IT MOVES ACROSS THE WIRE, YOU CAN SEE IT WITH EXTRAHOP

The ExtraHop platform enables security operations teams to keep tabs on all the communications and transactions in their environment. By analyzing their wire data, security teams can detect threats and get the context needed to answer what, where, when, and who for any situation.

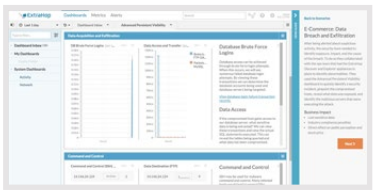
"ExtraHop shows what the applications are actually saying, not just who is talking to whom."

—Micah Rodgers
Senior Network
Security Engineer,
Murphy USA

ExtraHop enables security teams to analyze wire data, which is data-in-motion. This new data source effectively brings together the application and security teams to understand data patterns and determine what constitutes a potential threat. The outcome is a simplification of security and policy enforcement, and more effective detection of previously unknown threats.

MAINTAIN CONTINUOUS AND PERVASIVE VISIBILITY

- Automatically detect new devices communicating on the network and what protocols they are using
- Drill down to specific devices and examine lateral activity
- See the geographic location of requests for FTP, HTTP, and more
- Track and alert on anomalous privileged account activity
- Create event triggers to identify data exfiltration attempts
- Audit TLS/SSL certificates and spot weak ciphers to ensure secure in-flight encryption



DETECT AND ALERT ON MALICIOUS ACTIVITY

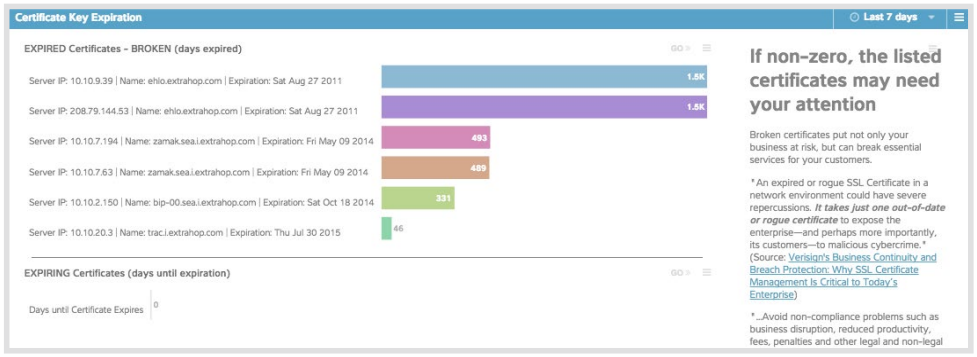
- Access-denied events for networked storage
- High and low-intensity brute-force attacks on authentication servers
- Data exfiltration from databases, file servers, and application servers
- Botnet command & control (C&C) activity that uses DNS TXT records
- Anomalous behavior across all tiers of your environment

TRY THE ONLINE DEMO!

Interested? Check out our free online demo. You can explore the interface for yourself and follow an incident-response scenario.

www.extrahop.com/demo

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.



ExtraHop's customizable security dashboards reveal potential vulnerabilities in security as well as augmenting your existing compliance capabilities with real-time visibility of your environment.

REAL-WORLD EXAMPLES

ExtraHop taps into the common element that ties every environment together—wire data—so that security teams can get comprehensive visibility into what is happening in their environment. The following examples show how ExtraHop has helped other organizations improve security.

AUTOMATED DETECTION OF HEARTBLEED VULNERABILITIES AND EXPLOITATION ATTEMPTS

The day of the Heartbleed announcement, a network and security ops team deployed the ExtraHop Heartbleed bundle for TLS Heartbeat Tracking, Dashboards, Client Identification and Geomaps. They watched malicious attempts to compromise their servers in real time, and immediately set blocking policies for those clients while they patched their vulnerable systems.

DETECTING DATA EXFILTRATION

A large government agency needed a way to identify the source of a data leak and detect any future data exfiltration. The security team used the ExtraHop platform to identify a specific machine with abnormal DNS activity as the source of the leak, and they now use ExtraHop as an integral part of their security monitoring and analytics.

TLS/SSL MONITORING

A large web hosting company used ExtraHop to continuously monitor SSL traffic between the load balancer and the backend servers, and fire off alerts if any traffic was not properly re-encrypted.

BYOD: MOBILE MONITORING & NETWORK OPTIMIZATION

A global enterprise tech company used ExtraHop's auto-discovery and application activity mapping to quantify "bring-your-own-device" (BYOD) activities on secure and guest networks, determining which applications were being accessed and implementing appropriate security controls.

SECURITY/ENCRYPTION AUDITING

A large enterprise with both incoming and outgoing SSL traffic used ExtraHop to view the entire set of SSL behaviors on their network, so they could see which certificates were being used, identify weak cipher suites, and set concrete steps for remediation.

BANNED PORTS, PROTOCOLS, AND SERVICES

A federal government agency used ExtraHop to monitor all connections that are banned per policy, such as protocols that transfer data unencrypted (FTP, telnet, SNMP, Gopher, etc.).

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