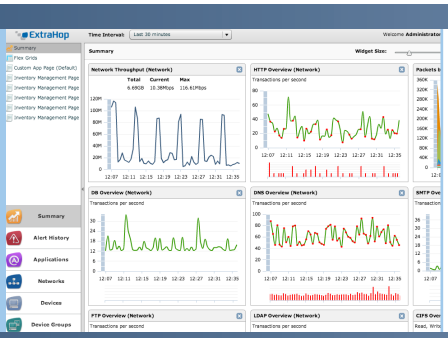
ExtraHop



The ExtraHop Security and Compliance Solution for Healthcare

Gain the IT Operational Intelligence Needed to Identify Threats, Prevent Data Leakage, and Simplify HIPAA Audits

Through noninvasive analysis of wire data, ExtraHop enables healthcare IT teams to easily flag problems, track anomalous events, and prove that their compliance measures are enforced. ExtraHop's security and compliance solution is extensible, allowing organizations to add additional metrics but includes difficult-to-monitor metrics out of the box:

- SSL transaction rates, ensuring all PHI data is encrypted while in flight.
- Expired or weak SSL certificates and ciphers, ensuring strong encryption is in pervasive use.
- Data passing over printer and USB channels in VDI environments to ensure locked down environments are in fact locked down.
- File access reporting to ensure protection of PHI, including tracking by user, file path, name, frequency, data rates, and performance.
- High- and low-intensity brute-force attacks on authentication servers.
- Data exfiltration through DNS TXT records—a common means to extract PHI.
- Superuser account activity, ensuring only those authorized to access databases are doing so.

ExtraHop provides a more efficient and effective way for healthcare IT teams to take care of security and compliance tasks demanded by HIPAA and HITECH. By analyzing all communication on the wire, ExtraHop provides the visibility needed to prevent data leakage, identify threats that IPS/IDS will not, ensure adequate encryption, and prove compliance during audits. ExtraHop's wire data analysis can easily be integrated with SIEM vendors or other log file or machine data analysis systems.

Monitor Unauthorized Access to Patient Data

ExtraHop passively analyzes all transactions passing over the wire so that IT teams have a complete and immediate record of database, storage, and directory services activity per user and client.

- Generate alerts based on failed directory services login attempts.
- Monitor unauthorized access to published applications according to group policy.
- Track unauthorized access to sensitive data on specific storage partitions.
- Know if users pass data over USB and printer channels in locked-down VDI environments.

Identify Threats That You Do Not Have an IDS Signature For

ExtraHop augments IDS/IPS by providing contextual visibility, including geographic, historical, and cross-tier data, so that IT teams can easily identify and stop suspicious activity.

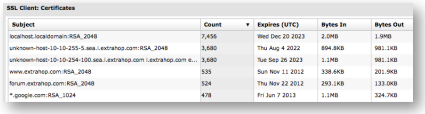
- View dynamic geomaps that include performance metrics and color-coded alerts with associated client IP addresses.
- Identify suspicious activity by viewing historical trends, including up to a full 30 days of lookback.
- Understand the context of an event by viewing correlated web, VDI, database, storage, DNS, and LDAP communications.

Simplify HIPAA Compliance Audits

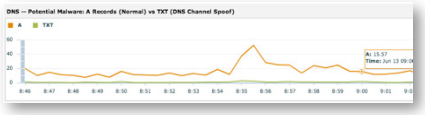
On average, HIPAA audit and assessment consulting services take between one and four months and cost between $150,000 and $480,000 for a one-time event. This is not only costly but takes scarce IT staff from other important projects. With complete records from ExtraHop, IT teams can easily prove compliance with key requirements.

- Show all SSL transactions to prove continuous encryption in flight and to ensure compliance for certificate keys being used throughout the entire environment, including their expiration date and cipher and key strength.
- Verify that all systems that should be using encryption are in fact doing so.
- Generate reports showing all reads and writes by user for sensitive directories.
- Track superuser activity across all databases.

Unlike IDS/IPS that use signatures, ExtraHop identifies threats by providing healthcare IT teams with the context—trends and real historical activity.



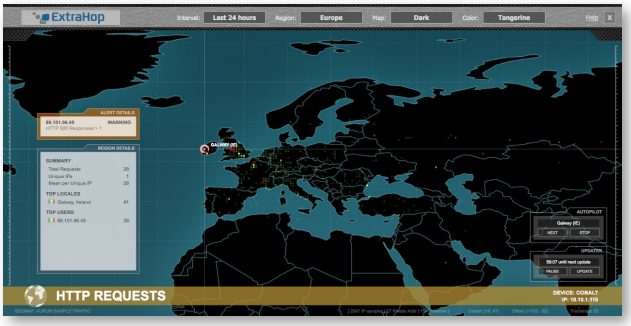
ExtraHop enables IT teams to easily audit their SSL encryption, including key strength and certificate expiration.



ExtraHop monitors TCP/IP tunneling through DNS by comparing regular A record volume with TXT record volume.

Get the ExtraHop Security and Compliance Solution Free with the Discovery Edition

The security and compliance solution works for the ExtraHop Discovery Edition. Download your free virtual appliance at www.extrahop.com/discovery.



ExtraHop reveals the geographic location of users, including color-coded alerts for errors and other events.

The ExtraHop platform is open and extensible, enabling healthcare IT teams to create additional custom metrics, alerts, and dashboards suited to their unique environments. Out of the box, the ExtraHop security and compliance solution covers six use cases that demonstrate the flexibility and power of the ExtraHop platform.

Locked-Down VDI Monitoring	In secure Citrix VDI environments, USB and printer channels are locked down to prevent leakage of patient data. ExtraHop provides a continuous audit of these measures by flagging all data passing over protected channels along with user and client details.
SSL Encryption Auditing	Verifying encryption is up to date and being used traditionally requires verbose logging on servers. ExtraHop enables IT teams to easily identify weak SSL keys and certificate expiration dates without logging.
Storage Access Monitoring	ExtraHop provides continuous monitoring of sensitive data on networked storage systems so that IT teams can see the client IP, username, and file path of all reads and writes. ExtraHop also tracks failed login attempts by unauthorized users.
Alerting for Brute-Force Attacks Against Authentication	ExtraHop identifies both high- and low-intensity attacks against authentication servers by monitoring LDAP success/failure rates, total failed attempts, and frequency of failed attempts per user.
Detection of TCP/IP Tunneling through DNS	Detect malware and data exfiltration attempts that use TCP/IP tunneling through DNS. ExtraHop breaks out DNS record types so that IT teams can compare normal A-records against irregular TXT records.
Superuser Account Tracking	Superuser accounts such as root and SA make it easier for malicious users to hide their tracks and cause damage. ExtraHop tracks superuser logins for MySQL with client and server details so IT teams can quickly take action.

About ExtraHop Networks

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop Operational Intelligence platform analyzes all L2-L7 communications between all systems, including full bi-directional transactional payloads. This innovative approach provides the correlated, cross-tier visibility essential for application performance, availability, and security in today's complex and dynamic IT environments.

ExtraHop