ExtraHop Protocol Modules

Fluent in the application protocols that your business runs on

The ExtraHop platform speaks the same language as the applications that run your business, and so can understand the content of communications as they occur. This real-time fluency at the application layer sets ExtraHop apart from competing products that only inspect data link or transport layer protocols.

Protocol Module Functionality

The following table lists the protocol analysis modules available for the ExtraHop platform as of September 2017. The modules offer varying levels of analysis. The most basic level of analysis is L7 classification. Application Inspection Triggers offer the ability for you to create a custom metric. Built-in metrics are those collected by the ExtraHop Discover appliance by default.

✓ = Included in base license ✚ = Add-on module

Triggers (No Built-In Metrics)

- ✚ ActiveMQ
- ✓ AJP
- ✚ DICOM
- ✚ HL7 (including FHIR and ICD-9/10)
- ✓ LLDP
- ✚ MSMQ
- ✓ Telnet

Triggers and Built-In Metrics

- ✚ AAA: RADIUS
- ✚ AAA: Diameter
- ✚ CIFS
- ✚ Citrix ICA
- ✓ DHCP
- ✓ DNS
- ✚ Database: DB2
- ✚ Database: Informix
- ✚ Database: Microsoft SQL
- ✚ Database: MongoDB
- ✓ Database: MySQL
- ✚ Database: Oracle
- ✓ Database: Postgres
- ✚ Database: Sybase
- ✚ Database: Sybase IQ
- ✚ FIX
- ✓ FTP
- ✓ HTTP/S
- ✚ IBM MQ
- ✓ ICMP
- ✓ Kerberos
- ✓ LDAP
- ✚ Memcache
- ✚ NFS
- ✓ POP3
- ✚ Redis
- ✚ VoIP: RTCP
- ✚ VoIP: RTCP XR
- ✚ VoIP: RTP
- ✚ VoIP: SIP
- ✚ SMPP
- ✓ SMTP
- ✓ SSH
- ✓ SSL
- ✓ WebSocket

Classification (No Triggers or Built-In Metrics)

- ✓ ARP
- ✓ GRE
- ✓ ICMP6
- ✓ IEEE 802.1X
- ✓ IKE
- ✓ IMAP
- ✓ IPSEC
- ✓ IPX
- ✓ IRC
- ✓ ISAKMP
- ✓ LACP
- ✓ L2TP
- ✓ MPLS
- ✓ NTP
- ✓ OpenVPN
- ✓ PCoIP
- ✓ RDP
- ✓ SNMP
- ✓ STP
- ✓ Syslog
- ✓ VNC

Built-In Metrics (No Triggers)

- ✓ HTTP-AMF
- ✓ DSCP
- ✚ iSCSI
- ✓ MS-RPC