ExtraHop Reveal(x) speaks the same language as the applications that run your business. Reveal(x) can understand the content of communications as they occur in real time, and use that understanding to detect threats, identify critical assets, quantify risk, and enable the SOC to execute rapid, effective investigations all the way down to forensic-level data inside application transactions and decrypted packets.

**PROTOCOLS SUPPORTED**

2TP  
AAA: Diameter  
AAA: RADIUS  
ActiveMQ  
AJP  
ARP  
BitTorrent  
CIFS  
Citrix ICA*  
Cryptocurrency mining protocols  
Database: DB2  
Database: Informix  
Database: Microsoft SQL  
Database: MongoDB  
Database: MySQL  
Database: Oracle  
Database: Postgres  
Database: Redis  
Database: Riak  
Database: Sybase  
Database: Sybase IQ  
DHCP  
DICOM*  
DNS  
DSCP  
FIX  
FTP  
GRE  
HL7 (including FHIR and ICD-9/10)*  
HTTP-AMF  
HTTP/S  
IBM MQ  
ICMP  
ICMP6  
IEEE 802.1X  
IKE  
IMAP  
IPSEC  
IPX  
IRC  
ISAKMP  
iSCSI  
Kerberos  
LACP  
LDAP  
LLDP  
Memcache  
Modbus  
MPLS  
MS-RPC  
MSMQ  
NFS  
NTP  
OpenVPN  
PCoIP  
POP3  
RDP  
RFB (VNC)  
Skinny (SCCP)  
SMPP*  
SMTP  
SNMP  
SSH  
SSL  
STP  
Syslog  
TCP  
Telnet  
VNC  
VoIP: RTCP*  
VoIP: RTCP XR*  
VoIP: RTP*  
VoIP: SIP*  
WebSocket*  

*Available as add-ons
Reveal(x) collects application layer metadata, via decoding and full payload analysis of more than 50 Layer 7 protocols, to derive 4,600+ features for user, application, and device activity. Our machine learning and detection models index this metadata for feature extraction as well as anomaly and other behavioral detections. The richness of this application-layer metadata enables Reveal(x) to detect malicious activities at each stage of the attack lifecycle that other products – which rely on flow-level information – cannot.

Of particular interest to SecOps analysts, Reveal(x) analyzes application-layer metadata for databases, Active Directory, DNS, web, SSL, and storage systems:

**DATABASE:** RDBMSs: Oracle, Microsoft SQL Server, MySQL, PostgreSQL, Informix, Sybase, and DB2. NoSQL databases: MongoDB, Memcached, Redis, Riak. Metadata extracted include transaction timing, table/user access patterns, query errors, SQL queries and responses, and system-level commands.

**IDENTITY AND ACCESS MANAGEMENT:** Active Directory visibility (includes LDAP, Kerberos, and DNS) for monitoring of privileged identities and service accounts to improve detection and facilitate audits. Reveal(x) extracts metadata including user/computer account activity, invalid or expired passwords, new privileged access, privileged access errors, DNS SRV lookups, plain-text LDAP binds, plain-text HTTP authentications, Unknown SPNs, and Golden Ticket detection.

**WEB TRANSACTIONS:** Full HTTP payload analysis of user activity, SOAP/XML, JSON, Javascript, APIs, etc. Extracted metadata includes URI, query parameters, host headers, and user agent, among others.

**STORAGE:** Metadata extraction for all NAS and SAN transactions (iSCSI, NFS, and CIFS) enables machine learning detections based on actual file details and equips security analysts to track file access patterns and detect ransomware activity by examining file extensions and WRITE operations.