Q-DLP®

The **Q-DLP**® (Data Loss Prevention) is a stand-alone, dedicated Data Loss Prevention tool (DLP), using **OpenDLP**, one of the most advanced open source Data Loss Prevention software packages available today. In addition to Data Loss Prevention, the **Q-DLP** includes tools to catch any attempts to alter files. We have also included **BRO-IDS**, an Intrusion Detection System (IDS) package, and **Brownian**, a web GUI for **BRO-IDS**. The **Q-DLP** is intended to complement the other Quantalytics network security appliances to help provide greater in-depth network defense. However, the **Q-DLP** may be used on a stand-alone basis. It is ideal for PoS (Point of Sale) networks.

Q-DLP Hardware Specifications:

- 108 mm x 64 mm x 26mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load: 8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

The **Q-DLP** includes:

OpenDLP - **OpenDLP** (Open Data Loss Prevention) is an open source, centrally managed, massively distributed data loss prevention tool. It operates both agent and agent-less. With suitable Windows, UNIX, MySQL, or MSSQL credentials, **OpenDLP** can simultaneously identify sensitive data at rest on hundreds, or even thousands of Microsoft Windows systems, UNIX systems, or MySQL or MSSQL databases. It uses a centralized Web management interface. Sensitive data can be credit card numbers, Social Security numbers, or any other user-defined sensitive data.

OpenDLP consists of two components: (1) A web application to manage Windows agents plus Windows and UNIX database agentless scanners. (2) A Microsoft Windows agent to perform accelerated scans on up to thousands of systems simultaneously.

Contact: Richard Avery
646-449-7810
Q-DLP@quantalytics.com

Quantalytics. In-depth network defenses.

Because of **OpenDLP**'s extraordinarily rich feature set and the interface with the **Q-Log®** for log analysis, we recommend visiting our web site at www.quantalytics.com for a far more detailed description.

- **Bro-IDS** – **Bro-IDS** is both a signature and anomaly-based IDS package. **Bro-IDS** examines all network events (e.g. FTP, HTTP) and then, using its Policy Script Interpreter, provides insight into the legitimacy of the events. **Bro-IDS** includes Bro-Script, its own scripting tool, to create custom rules and analysis. **Bro-IDS** interfaces with the **Q-Log®** for monitoring and analysis of its intrusion detection logs.

- **Brownian** – **Brownian** is the Web interface for **Bro-IDS**.

- **Xplico** - **Xplico** is a leading open source package for real time network packet capture and forensic analysis. In the event **Bro-IDS** shows suspicious activity, network administrators can capture and examine in depth real-time traffic for deeper analysis of suspicious network traffic. In addition to packet inspection, **Xplico** allows for reconstruction of the actual traffic. E.G. E-mails, texts, IM's, pictures, etc.

- **Webmin - Webmin** is used for network appliance housekeeping and network configuration, including WiFi.

- **HA Proxy** – **HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-DLP** servers may be linked for automatic failover or load balancing for coverage of extremely large networks. Setup and administration is done through **Webmin**.

- **ModSecurity®** – **ModSecurity®** (**ModSec**) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. **ModSec** is used to harden the **Q-DLP**'s built-in Apache web server and prevent conceivable attacks.

Contact: Richard Avery
646-449-7810
Q-DLP@quantalytics.com

- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **ClamAV®** – **ClamAv®** is the leading open source anti-virus package.

The **Q-DLP** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.). Intrusion detection can be set up on either network interface.

The **Q-DLP** is also available as a Virtual Machine.

The **Q-DLP** is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. The **Q-DLP** network appliance can be integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-DLP** network appliance can also be integrated with the **Q-Log®** network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Contact: Richard Avery
646-449-7810
Q-DLP@quantalytics.com

Quantalytics. In-depth network defenses.