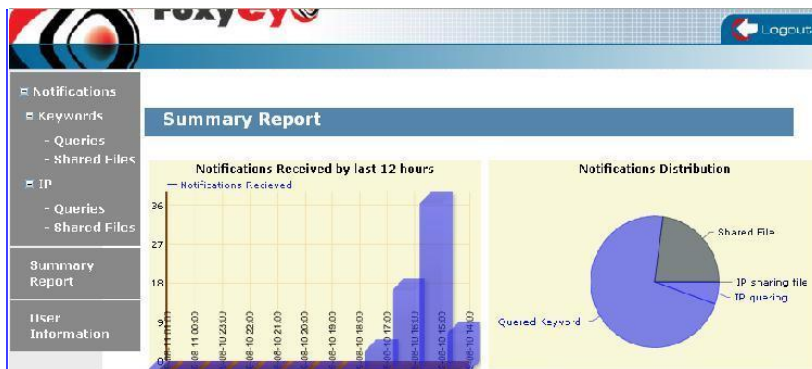


FoxyEYE Specification



註解 [JS1]: The screen shot is not clear.. Would it be ok in print??

註解 [KT2]: This may not be completely true. It is possible to block Foxy traffic by restricted access to the Foxy Web Cache server, which is used when a Foxy client first join the Foxy network. However, it is correct to mention that the file sharing traffic of Foxy is difficult to be blocked (via blacklisting firewall rules), just like all other P2P file sharing network, as they use dynamic port numbers.

註解 [KT3]: It seems that this point is the same as the previous one.

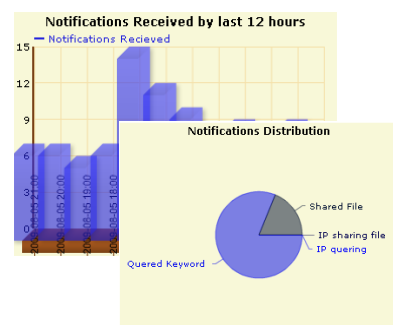
註解 [KT4]: Some generic comments for this section. The logical flow of this section is not too clear. Maybe can rewrite as follow?

1. The issues of Foxy file sharing (data leakage, example, etc)
2. The difficulties in blocking & detection in corporate network.
 - Initial traffic to Foxy Web Cache servers use HTTP traffic
 - difficult to be detected without in-depth network analysis
 - may be able to block known web cache server hosts, but require continuous effort to maintain the known server list
 - Dynamic port usage → difficult to block in network firewall using “blacklisting” approach
3. Alternative solution (monitoring in the Foxy network)
4. Name our product

FOXY is a P2P software for file sharing which is very popular in Hong Kong, Macau, China and Taiwan. Since 2006, there have been several sensitive information leakages cases in Taiwan and Hong Kong that happened through the FOXY network. Some of these cases are high profile information leakages that involve celebrities, as well as sensitive information from government agencies.

Once a file is published, and after the first copy has been replicated on a peer, it is impossible to stop the leakage. The best solution is obviously to avoid the initial leakage. However, it is very difficult to block the usage of FOXY within organizations’ network due to three reasons – 1. FOXY clients can connect to FOXY network using a wide range of port numbers, thus it is very difficult to block in network firewall using “blacklisting” approach; 2. Initial traffic to Foxy Web Cache servers uses HTTP traffic, thus a quick detection of connection is difficult, unless through the use of deep packet analysis; 3. Even though known web cache server hosts are blocked, continuous effort is required to maintain the known server list. Also because of the three reasons listed above, there is still no software that can effectively detect the use of FOXY within organizations’ network or monitor the FOXY network for the possible leakage of sensitive files. **FoxyEYE** is the first software solution that is dedicated to detect the leakage of files through FOXY network.

FoxyEYE



FoxyEYE is our solution to can allow organizations to monitor their network for the possible leakage by FOXY. Through alerts, **FoxyEYE** can quickly detect any information leakage and allow the user to react to it quickly. Through the means of IP and filename monitoring, **FoxyEYE** will raise alerts once they are detected on the Foxy network. Organizations can make use of this by monitoring IP or filename related to them. Using such measures, the organization could easily notice any leakage and react fast enough to stop the spread of sensitive information within the FOXY network.

Features

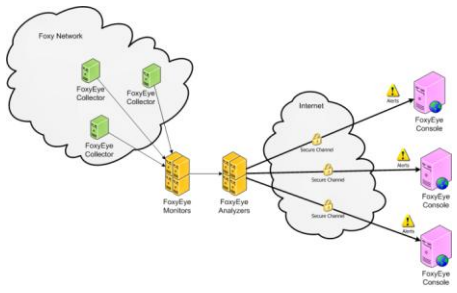
1. Detect the IP address of any connected FOXY client within the organization’s network
2. Monitor the FOXY network for possible sensitive files leakage and sharing among FOXY users.
3. Allow users to specify the list of files that need to be monitored.
4. Alert users for abnormal activities through **FoxyEYE** interface.
5. Detect the leakage of any file with sensitive keywords by using passive monitoring techniques.

Benefit

1. Enable users to monitor and detect unauthorized use of FOXY within networks.
2. Allow users to detect the shared sensitive files on the FOXY network, monitor the defined IP address range and specified file keywords.
3. Allow users to promptly spot any file leakage
4. Provide historical records for monitored files and shared file information

IP Detail			
Detail of "w.x.y.z"			
Country: N/A			
- Region: N/A			
- City: N/A			
www.ipaddress.com/			
ip	datetime	protocol	keyword
w.x.y.z	2009-08-11 09:00:10	QQ	cross game 19 mmb
w.x.y.z	2009-08-10 17:35:50	QQ	羅家禧
w.x.y.z	2009-08-10 16:04:53	QQ	laine garry hudson
w.x.y.z	2009-08-10 16:03:02	QQ	何尚賢
w.x.y.z	2009-08-10 16:00:02	QQ	潘曉

Software Architecture



FoxyEYE monitors are effectively silent users that collect information from the FOXY network. Through the means of IP and filename matching, it can determine whether the monitored IP addresses are connected to the network and whether sensitive files are being shared among FOXY users. As a silent user, **FoxyEYE** collectors listen to the FOXY network without providing any data/information for other FOXY users. The collected information is sent to a local **FoxyEYE** monitor for keyword/IP scanning. All these matching are done inside the

local network to ensure that the keywords/IP that are monitored stay within the network. Using passive scanning techniques, no active searching on the FOXY network is performed. Statistical data in the **FoxyEYE** solution are computed using **FoxyEYE** analyzers with the information from the monitors. Lastly, **FoxyEYE** consoles are installed to the end-user's computers. Such consoles facilitate the raising of alerts when abnormalities arise.

Further details

Tailor Made version for **FoxyEYE** could also be provided by request. For further details, please contact **Marketing Team** (marketing@ewalker.com.hk) or logon to www.ewalker.com.hk

Limitations	1. FoxyEYE is a monitoring software, thus no service would be provided for preventing or stopping any leakage from the network; 2. FoxyEYE cannot 100% guarantees the detection time of leakage; .3. eWalker reserves the right to disprove any keyword or IP address being monitored by FoxyEYE ; 4. FoxyEYE users can only access to FoxyEYE console user interface.											
Versions	<table border="1"> <thead> <tr> <th>Version</th> <th>Keywords Monitored</th> <th>IP Monitored</th> </tr> </thead> <tbody> <tr> <td>Basic</td> <td>10</td> <td>15</td> </tr> <tr> <td>Professional</td> <td>20</td> <td>255</td> </tr> </tbody> </table>	Version	Keywords Monitored	IP Monitored	Basic	10	15	Professional	20	255	<p>There are different versions available and pluggable service updates would be provided as additional service from time to time.</p> <p>Hosted Version is provided to clients so that the whole solution is hosted by eWalker and clients can deploy minimal recourses. All the statistical data would be provided to clients through web console. Software Version is also provided for clients so that all data would be collected through our application console.</p> <p>Additional Services include: Additional IP range monitoring, Additional keyword monitoring (per 10 keywords), Customization, Training, Extra maintenance, Technical Support and Installation</p>	
Version	Keywords Monitored	IP Monitored										
Basic	10	15										
Professional	20	255										
System Requirement	<p>Hosted Version: Flash player 10; Internet Explorer 7.0/Firefox 3.0 or above; Internet connection</p> <p>Additional Requirements for Software Version: Windows XP Professional, Windows Server 2003 or above; Microsoft Internet Information Server (IIS) 5.1; NET Framework 3.5</p>											