Watchful Software keeping an eye on data protection

Analyst: Javvad Malik 4 Dec, 2013

Despite maturing security technologies, information losses occur on an almost daily basis. These happen for a variety of reasons ranging from external attackers, malicious insiders, carelessness or apathy.

To protect data, companies usually employ data leak prevention (DLP) or information rights management (IRM) offerings. Some may view DLP and IRM to be mutually exclusive technologies; however, Watchful has tried to bring the best of both worlds into the fray with its RightsWATCH offering.

The 451 Take

We've previously written about the challenge of secure document collaboration. We like the approach of combining the best from DLP and IRM technologies that Watchful has adopted. However, there is a vast array of vendors offering to protect enterprises from data losses and making its presence known in a market that may have had some poor experiences with earlier deployments of DLP or IRM may be the bigger challenge for the company. Nonetheless, by building up some successful deployments, Watchful should be able to install confidence in its approach.

Context

Portugal-based Watchful Software is a spinoff from Critical Group, where the initial product development was undertaken. Since 2012 the company has been independent under the leadership of CEO Charles Foley. In November 2012, the company received venture funding from Critical Ventures, the vehicle of Critical Group for seed and early stage investments.

The growing company has just under 25 employees, the majority of whom are employed within R&D. Watchful Software has ambitions to add to its sales and marketing headcount going forward in order to drive growth.

Products

RightsWATCH is Watchful Software’s data security offering that protects individual files. The product leverages techniques from both IRM and DLP in one product. The company believes this method combines the strengths of both techniques but without the weaknesses.

Like most DLP technologies, RightsWATCH has its own information security policy schemes, which can be tailored to specify what level of protection should be applied to various types of data. However, if a company doesn’t have a defined policy, RightsWATCH can create a policy by observing normal usage and building a baseline profile. The information the product gathers can be leveraged in its monitoring function by providing reports on how sensitive information is being accessed, including sysadmin activities. RightsWATCH can integrate with AD for user enrollment and policy enforcement. It can also leverage MS RMS encryption to undertake the heavy lifting.

Protection of files is based on the scope; i.e., whether the information should remain internal to the company or a department and the level at which users within that particular scope are required to be. This combination of scope and levels gives the ability to assert fine-grained control over the files, allowing organizations to protect information on a need-to-know basis.

When a user creates a new document or email, depending upon the setup, RightsWATCH can auto-populate the scope and levels driven by policy-
based rules, which creates a no or minimal user interaction. Content-aware rules are also present, which will be triggered based on certain keywords. For example, the mention of a confidential project name can trigger a content rule to raise the level of protection on the file.

Companies can make some rules non-mandatory, thus allowing users to manually override rules by virtue of digitally signing a disclaimer. Aside from full encryption, RightsWATCH can also automatically insert watermarks to documents throughout all Microsoft office documents and some third-party applications too, such as Adobe PDF files.

There is also an element of BYOD support that RightsWATCH can provide by extending the functionality of data classification and IRM on Android, iOS, BlackBerry and Windows phones. The access controls are maintained and in the event a device is lost, stolen or an employee departs, all corporate files protected with RightsWATCH can be remotely deleted.

**Competition**

The document protection market has always been a buoyant one and it seems to be getting more crowded by the day. Watchful Software will be competing against a whole slew of protection technologies, DLP and IRM vendors. These will include vendors which offer secure collaboration functionality such as Soonr, Mezeo Software, Teambox, Huddle.net, Egnyte and Seclore.

Additional competition will come from mail encryption like TITUS, Moxier and NitroDesk’s TouchDown. Also not to be discounted are IRM vendors such as GigaTrust, Covertix, Avoco Secure, Trustwave (BitArmor systems), Zafesoft and the like.

**SWOT Analysis**

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>The combination of the best parts of DLP and IRM technologies gives Watchful Softer a good baseline from which it can build up customer success stories and additional features.</td>
<td>There is a certain stigma associated with DLP and IRM technologies from the past where deployments have failed or not been as fruitful as companies have desired. Watchful Software will need to convince perspective customers that history won’t repeat itself.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>By identifying and targeting the right enterprise customers, Watchful Software could plug the hole companies have with minimal additional investment, and gain market share in the process.</td>
<td>There are a plethora of competing technologies in the document security space. In particular, the ones that focus on securing data in the cloud will all be jostling to be the enterprise product of choice.</td>
</tr>
</tbody>
</table>

This report falls under the following categories. Click on a link below to find similar documents.

**Company:** Watchful Software

**Other Companies:** Adobe, Avoco Secure, BitArmor, BlackBerry, Covertix, Critical Group, Egnyte, GigaTrust, Huddle.net, Mezeo Software, Microsoft, Moxier, NitroDesk, Seclore, Soonr, Teambox, TITUS, Trustwave, Zafesoft

**Analyst(s):** Javvad Malik

**Sector(s):**
- Security / Encryption / General
- Security / Other