

**PKWARE focuses on compliance for encryption-based  
DLP remediation rollout**

**Analyst: Steve Coplan**

This quarter, **PKWARE** will launch a stand-alone SecureZIP encryption product for data loss prevention (DLP) remediation that involves integration of output from DLP systems into its SecureZIP encryption schema in order to lock down sensitive data and files. Once the DLP system has identified data at rest as sensitive, the PKWARE product can automatically (with programmatic integration in place) encrypt the target file and then replace it with a SecureZIP file, removing the need for manual remediation and an interregnum where the data is still in clear text. The product also ties into corporate user stores (typically **Microsoft** Active Directory) and extracts metadata in order to determine the data owner and, by extension, to whom the encryption keys should be distributed. In tandem with the release of its DLP remediation product, PKWARE has also announced certification with **Symantec's** FlexResponse API for its DLP systems and rolled out an outbound API that third-party DLP vendors can write to in order to invoke the remediation capabilities.

As we have noted before, DLP technology has proven effective in the areas of discovery and classification – especially in the area of data with a consistent internal format that falls under compliance mandates – but less effective in serving as a means of translating that output into enforcement frameworks and aligning the enforcement with an existing business process contingent on access to the data. This is the well-established need that PKWARE (alongside several other competitors) is looking to address. PKWARE is targeting a tightly-defined use case at this point – data at rest that falls under compliance mandates – for its remediation capabilities. However, if we draw the dotted lines to its SecureZIP footprint within enterprises, and assume that it can build some momentum for its northbound API strategy, the potential does exist for the company to strike a balance between user-driven file-encryption policies and a bottoms-up classification process for identifying and locking down data and information.

**The 451 take**

PKWARE is hardly the first vendor to implement integration with the Symantec FlexResponse API or similar APIs offered by Symantec DLP competitors. The development of outbound APIs by the DLP vendors points to a longstanding acknowledgement that there was a need to tie DLP intelligence to a more flexible enforcement framework informed by business-process requirements rather than rely on native encryption capabilities. Where PKWARE is forging into new territory is by publishing its own API, even as it creates the potential for integration with its encryption footprint on enterprise endpoints and servers. There is an aspiration here to broaden its encryption footprint, but the real opportunity lies in transparently enforcing policies that combine machine classification and user input to balance security, compliance and availability.

PKWARE has released a stand-alone remediation product, SecureZIP for DLP, providing encryption for data at rest that is classified as sensitive by DLP discovery, scanning and classification processes. Sensitive data in this context is largely understood to be data that falls under compliance mandates, including social-security numbers, credit card numbers and personally identifiable information. The intent here is to slot encryption into DLP policies and workflow, with SecureZIP for DLP automatically invoked based on policy settings. Once the file is encrypted within the SecureZIP schema, it replaces the original file in storage. SecureZIP for DLP is designed to extract file metadata and to integrate with Microsoft Active Directory (or other LDAP-compliant directories) in order to pinpoint the data owner (based on characteristics like group membership and roles), who, in turn, inherits responsibility for the encryption key, from a technical point of view, and accountability, from an operational point of view. If the process assigns ownership, but the identity is no longer a valid identity (since the employee has left, for instance), the PKWARE Contingency Key allows administrators to recover the encrypted data and reassign ownership.

Also, PKWARE has announced certification for the Symantec FlexResponse DLP API. In addition, PKWARE has developed its own documented API, which enables DLP vendors to call SecureZIP for DLP encryption in response to an alert or notification. Programmatic integration is a crucial element in facilitating automation and policy-driven automation. The API incorporates options for administrators to define the DLP policy settings and customize remediation options. Although automation of remediation is critical to ensuring that data subject to compliance mandates is encapsulated within a control framework, there's the potential for falling afoul of business processes – a perennial DLP implementation issue that PKWARE is also looking to address here.

After tailing off following the initial rush toward implementation of DLP technologies, which, in turn, catalyzed a spate of acquisitions, we have seen spending increase for DLP, and indications are that many enterprises have budget set aside for broader implementation. End-user spending intentions tracked in primary research based on in-depth interviews by our TheInfoPro subsidiary suggest that more than 50% of participants at both large enterprises and medium-sized enterprises intend to increase spending in 2012 over 2011 on endpoint DLP, and just under 50% on network DLP. And, while at least half of the large enterprises interviewed by TheInfoPro indicate that they intend to spend more on endpoint and network-based DLP, levels of implementation are still around 25% of the participants in the research wave. This discrepancy between spending intentions and implementation can be explained by the reality that, like most security products, DLP was designed to deal with a technology challenge – not primarily as a way of implementing more secure business processes.

However, as the reality of DLP has set in, we have also seen the gradual recognition take hold that DLP can't function as a silver bullet to stemming inappropriate or targeted data exfiltration. DLP, however, has proven to be a useful tool in generating visibility into the distribution of sensitive content through discovery processes and, as a result, defining the scope of compliance efforts. Also, we have seen enterprises extend classification efforts to expand the number of channels for monitoring of potentially sensitive data. Still, most organizations are wary of implementing the 'protect' element of DLP, since it can be disruptive to business processes. And the level of effort and investment in tuning DLP filters to bring down the rates of false positives can be prohibitive. One path organizations have

chosen is to alert, notify or report rather than block or encrypt data. Since this approach can have both poor security outcomes and fall afoul of compliance audits, the approach organizations have taken to resolve this challenge is to define a set of data that must be locked down and monitored for compliance reasons through a focused DLP implementation, and then look to remediation as the bridge between DLP and operations. This limitation was the impetus for Symantec developing its Symantec FlexResponse API, which was launched in 2009.

However, remediation is not without its challenges, too. In order to limit the disruption to business processes, many organizations will employ a manual remediation process, which leads to inefficiencies. Also, many organizations struggle with driving accountability into the process of handling data under compliance. Again, providing a mechanism to automate this process of encrypting data and assigning keys to the data owner through programmatic integration is a crucial structural requirement. PKWARE's integration with the Symantec API doesn't qualify as groundbreaking, but its plan to publish an outbound API so that DLP vendors can integrate with its remediation capabilities and then extend its existing encryption and compression footprint could ultimately drive broader and deeper DLP implementation. PKWARE also falls into the broader trend of greater orchestration at an enforcement level between data classification and access entitlements to address policy conformance and data exposure risk.

PKWARE has emphasized that the DLP remediation product can function on a stand-alone basis, with no dependencies on other SecureZIP components. However, since the product is interoperable with SecureZIP endpoints and servers, there is clearly the potential for the company to exploit its footprint. Again, PKWARE has set its focus on a bounded use case with broad applicability. However, since the products are interoperable, the strategy is clearly to encourage broader use of the product family. Here, the long-term opportunity is to balance machine-generated classification of data that must be locked down with user-driven classification of information that should be locked down, within the context of a shared, policy-based encryption schema and identity-driven key management exchange.

## Competition

The most obvious point of departure for mapping out the competitive landscape is to identify those vendors that have also certified to the Symantec FlexResponse server and endpoint APIs. When Symantec initially announced its FlexResponse server API program with the launch of version 10 of its DLP product in 2009, the first batch of vendors that signed on were **Oracle, Liquid Machines, GigaTrust** and **PGP**. Liquid Machines has subsequently been subsumed within **Check Point**, and PGP is now an operating division within Symantec, following its acquisition in April 2010. Symantec has spent some time on integrating PGP and the **GuardianEdge** full-disk encryption technology, with the intention to formulate a common key management schema and implementation processes. As Symantec's O3 project suggests, the long-term strategy is to tie encryption to access management initially, and to 'information-centric' security over time. This would suggest that, over the long term, Symantec will look to facilitate greater degrees of automation, but as a pragmatic course of action, is likely to continue to support the FlexResponse APIs.

Other vendors have implemented integration with DLP platforms – **Titus Labs**, for instance, has partnered with both **McAfee-Intel** and **Verdasys**. However, Titus' technology is aimed at resolving a different use case, specifically locking down content and files that are sent over email (and especially Microsoft Outlook). Also, while Titus can now incorporate machine-generated classifications into its enforcement, the company's philosophical emphasis is on user-driven classification. Titus' approach is ultimately contingent on the level of training and policy knowledge across the user population.

**RSA** offers its own DLP remediation product, alongside its DLP technology that is the outcome of the acquisition of **Tablus**. Also, Microsoft has a longstanding partnership and ongoing development alliance with RSA to more tightly integrate DLP with its Active Directory Rights Management Server so that files are automatically enrolled in the enterprise rights management framework.

Elsewhere, we have seen efforts by vendors to more tightly orchestrate DLP intelligence and access management. For instance, **CA Technologies** first coined the term 'content-aware IAM' – when it acquired DLP vendor **Orchestria** in early 2009 – to describe its strategy of concatenating DLP intelligence with access controls in a single policy statement. The company has made steady, if protracted, progress toward delivering on this vision. Likewise, **Courion** has an access governance partnership in place with Courion through its FlexResponse initiative to integrate its policy controls and encryption into a workflow triggered by data-classification parameters. Also, information rights management vendors like **Covertix**, **InDorse Technologies**, **Zafesoft**, **Pawaa Software**, **WatchDox** and **Secure Islands** will partner tactically with DLP vendors for file-level protection, monitoring and access controls.

Symantec remains the most visible player in the DLP market, especially in the realm of storage and endpoint DLP, followed by Intel-McAfee. Outside of the two large security vendors, a number of vendors divvy up a still fragmented market across a number of channels, with **Sophos**, **Websense** and **Trend Micro**, as well as pure plays like **Code Green Networks** and **Wave Systems-Safend** in the midmarket, and Verdasys at the high end, filling out the picture.

Reproduced by permission of The 451 Group; copyright 2010-11. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to: [www.the451group.com](http://www.the451group.com)