



Advisory Report

Data-centric Access Control



Andrew Braunberg

Research Director, Enterprise Networks and Security

September 28, 2009

■ Summary

Data loss prevention is a relatively small but strategic security market segment. Data loss prevention (DLP) is a key component in enabling a broader shift to data-centric security, which would place the protection of sensitive data at the center of security strategies. This has always been a key goal of security strategies and the shift is more in means than ends. Several interesting integration trends are currently emerging in the DLP market with the relatively recent interest from identity management and information rights management vendors to integrate data discovery and classification features into their suites.

The goal of delivering data discovery, classification, and control on top of fine-grained entitlements management or digital rights management should resonate well with enterprise customers as they begin to consider the need for more comprehensive risk management solutions. This tracks well with the more general trend of enterprise customers to work with a smaller number of more strategic security providers. DLP technology will find many homes, and we are already beginning to see the technology integrated into multiple suites (e.g., threat management suites), but the integration with identity management and rights management products is perhaps the most exciting because of the functionality it enables and the vendors it brings more directly into the security markets.

■ Current Perspective

The data loss prevention market remains relatively small (\$300 million or so projected for this year), but the technology has had a much larger impact in reorienting the security market toward a more data-centric approach to information security and compliance management. The ability to discover and classify sensitive information quickly and automatically is a foundational capability that can significantly enable and extend the functionality of threat management, identity management, and enterprise rights management suites.

The DLP market has been driven to a large extent by the compliance requirements. Although DLP is not explicitly mandated in any major compliance legislation, it is often seen as a best practice for identifying and protecting sensitive data. We expect the continued tighten-

Report:

**Data-centric
Access Control**

Enterprise Security

ing of existing compliance frameworks, such as the revised HIPAA requirements and the broad enactment of breach notification laws in most U.S. states, to continue to drive DLP deployments. Several DLP vendors have targeted the SMB market segment and we believe that underserved market will find the same benefits in the technology as enterprise customers have traditionally. However, we expect European and Asian enterprise customers to continue to lag their North American counterparts in interest and deployment.

DLP vendors began to attract the attention of traditional threat protection vendors a couple of years ago and early market consolidation was driven by McAfee, Symantec, Trend Micro, and others. The desire to integrate DLP functionality, particularly data classification, into endpoint suites and gateway products was a driver of this wave of acquisition activity. More recently, we have seen interest from identity management and rights management vendors. Microsoft, which plays in both camps, was one of the first proponents of this type of integration. In December 2008, it announced a partnership with RSA, the Security Division of EMC, to integrate RSA's DLP Suite 6.5 with the Active Directory Rights Management Services (RMS) within Windows Server 2008.

With RSA's DLP Datacenter and DLP Endpoint Discover, users can find sensitive data at rest and apply RMS controls based on a central set of policies. The combined solution also provides protection of data at rest throughout the infrastructure based on content awareness from RSA DLP and identity awareness from RMS. RSA's DLP 6.5 release integrated AD Group functionality in DLP Network and DLP Endpoint Enforce. Microsoft's rights management and DLP strategy dovetails nicely with several initiatives it has underway in the broader identity management market. For example, Microsoft's Geneva claims-based identity framework, which builds on Microsoft's CardSpace user-centric identity initiative, could easily consume RMS/DLP policies as additional privileges/claims.

Another important player in this convergence is CA, which acquired DLP vendor Orchestria in January 2009. CA has been a long-time leader in the identity management space. It plans to integrate the Orchestria technology with entitlements management technology that it acquired from IDFocus and Eurekify to add data-level role-based provisioning to its Role and Compliance Manager product. This integration work is currently underway, but some early work has been completed. CA DLP does integrate with LDAP directories and can consume user attributes. DLP can also make lookup calls out to other systems (such as Active Directory) when analyzing end-user activities. This enables DLP to determine whether a certain activity is a violation based on a user's title, department, region, etc.

We expect other identity management players to make similar moves. Oracle, in particular, is well positioned to be a major driver of the broader integration of DLP features into broader software suites. Oracle is a leading identity management suite provider. It has also moved into the enterprise rights management market with the acquisition of Stellent, which had acquired SealedMedia. Oracle is also expanding its footprint in the database activity monitoring space, which also has common interest with DLP. Other vendors that have a strong presence in the identity management (and systems management) markets are IBM and Novell. We expect both to develop DLP strategies as well. In general, identity management vendors will be extremely competitive long term as providers of DLP functionality, because they sell to the right buying center and, more importantly, data-level access control is a natural extension/evolution of IdM suites.

There are definitely easier integration projects than merging identity management and DLP. Adding DLP to integrated client security and secure messaging solutions, for example, is simpler and farther along today. However, marrying DLP to devices or communications channels is inherently a stop-gap measure. Data access policy needs to be tied consistently

Report:

**Data-centric
Access Control**

Enterprise Security

and irrefutably to individuals or, in enterprise environments, potentially to groups (based on roles). Or, obviously, policy needs to be tied directly to the data. This is where the enterprise digital rights management vendors come into the picture. As mentioned earlier, Microsoft fired the first shot. This was followed almost immediately by a “me too” announcement from Liquid Machines and McAfee. That partnership has yet to bear fruit and McAfee has more recently (just this week actually) announced a partnership with Adobe. Adobe sees Microsoft as its chief competition in the rights management space and the partnership with McAfee, while defensive, is also clearly strategic. Unfortunately, details are currently absent beyond a commitment to integrate Adobe’s LifeCycle Rights Management ES software with McAfee’s DLP technology. An integrated solution is expected to be available early next year that will be targeted at protecting data on enterprise endpoints. Liquid Machines actually promises more detail on jointly available products sometime later this year. Interestingly, Liquid Machines uses an open approach, which it claims will support Microsoft’s platform called Rights Management Services (RMS). Through its DLP integration, Liquid Machines will enable Microsoft RMS customers to leverage security technology from vendors such as McAfee.

It is interesting that the ability to deliver continuous, automated data discovery and classification through DLP integration may provide the usability that enterprise rights management systems need to finally move into the mainstream. Compliance requirements, which have been such an important driver in building awareness and growth in the standalone DLP market, will increasingly drive the integration of DLP features into these broader suites as truly comprehensive and fine-grained access control becomes obtainable.

Recommended Actions**Recommended Vendor Actions**

- We are excited about the integration of data classification technology into a host of broader suites, but DLP will remain a standalone market for as long as customers are willing to pay a premium for the functionality. This will remain the case until data classification analysis can be seamlessly consumed and used as part of a broader access control policy framework.
- The general concern with the existing DLP/IdM/ERM integration announcements is a lack of firm detail. The degree of integration or even firm product roadmap information is often lacking. Vendors such as CA, McAfee, Microsoft, and RSA should continue to tighten commitments to announced deliverables.
- McAfee and RSA have been the most aggressive DLP vendors to partner with access control vendors. Pure-play DLP vendors, particularly those that target the enterprise and mid-market segments, should be actively pursuing partnerships with vendors in these spaces.
- Similarly, identity management suite vendors that have not yet announced strategy for integrating DLP functionality into their suites should do so. We would expect announcements from IBM, Novell, and Oracle by the end of this year or early next year.
- These efforts to bring out-of-control data into a business-manageable form are being mirrored in the archiving, legal discovery, and document management markets. Companies in the DLP market should look into efforts in these markets and consider merging their approaches to what is a thorny problem for IT in every market segment.

Report:**Data-centric
Access Control**

Enterprise Security

Recommended User Actions

- Customer options for deploying DLP functionality within broader access control suites is currently limited but, as discussed, several leading vendors are busy bringing joint solutions to market. Enterprise customers should, however, be thinking about data protection as a policy management problem. Comprehensive policy should support fine-grained user and data attribute-based access control.
- Existing customers of Microsoft Directory Rights Management Services and RSA DLP should be exploring the benefits of joint deployments. CA identity management customers and McAfee DLP customers (as well as Adobe and Liquid Machine customers) should be looking for more information from those vendors with regard to availability of their respective integrated products.