Sales Accreditation Battlecard

Understanding McAfee Data Loss Prevention

Created: November 2013 **Internal and Partner Use Only**

Feature	Advantage	Customer Benefits	Differentiation
Capture Technology	Provides a historical record of all data leaving the enterprise without impacting performance of business data and traffic	• Helps you build DLP policies faster and better by giving you visibility into how your sensitive information is used across your enterprise.	• Symantec claims to solve this need using "Vector Machine Learning", but their technology requires collection of perfect samples in advance to train and tune the DLP policy engine. Using McAfee's Capture technology, you don't have to know everything before protecting and deploying efficient DLP policies.
Data Classification	Classifies large amounts of data residing on servers and file shares through rapid data inventory, categorization, and automated remediation.	• Helps you save time and resources by categorizing large amounts of unclassified data so only relevant files are examined and remediated. Don't waste time and resources on irrelevant data!	• RSA claims their "scalable" DLP solution addresses the "big data" problem. But their solution requires crawling through every server, which is time and resource intensive. With McAfee's Data Classification, you can do rapid inventory using meta-data only, and use unique McAfee DLP concepts to accurately identify relevant files to remediate first.
Location and Application Tagging	Tags all files from protected locations or applications. When a file is copied onto an endpoint, it retains its security settings through manipulation such as clipboard and renaming.	• Helps you efficiently and easily set up robust DLP policies based on location and application type. Gives you faster protection for data without crawling servers and fingerprinting every file.	• No competitor can match this level of sophisticated tagging.
Virtualization Support	Supports Citrix and VMware terminal servers, Citrix XenApp, Citrix XenDestop (VDI), VMware View (VDI) and Microsoft Terminal Server.	• Monitors and intercepts all user sessions at a **per-user** policy level, allowing flexibility and better control of data flowing to the terminal. For example, one user can print from a session on a server, but a second user with different access levels on the same server cannot.	• While other DLP vendors support VDI, they only have a single policy enforced on these terminals – meaning that one policy must apply to all users, regardless of role or business requirements. Only McAfee offers the per-user policy.
Security Connected Platform	McAfee DLP alerts and events can be correlated with other McAfee security events within McAfee ePO. This enables seamless integration with McAfee device control and endpoint encryption solutions.	• Integrations provide visibility and control and a 'single pane of glass' across other McAfee security products. This saves time and cost through vendor consolidation, and reducing the number of consoles you need to deploy, learn and manage.	• No competitor has the capabilities of McAfee's ePO platform and its integrated security strategy.

Sales Accreditation Battlecard

Objections	McAfee Response
“Symantec has one console to manage its DLP solution.”	Symantec DLP actually requires multiple consoles and agents to deliver its full DLP solution. In addition, it also requires a separate Oracle and SQL Database, leading to higher cost and complexity. McAfee DLP’s solution consolidates agent and database requirements, making it more cost effective and simpler to deploy and manage.
“Symantec uses Vector Machine Learning technology which is similar to McAfee's Capture technology.”	Symantec is using a technology, Vector Machine Learning, which is unreliable and has been shown to fail when used by other vendors in the past. The flaw in Vector Machine Learning technology lies within the manual process of keeping the training database updated which can cause error and larger false positives.
“We already have Symantec DLP on our endpoints.”	You may have invested in this endpoint solution, but over time, it will cost you more and deliver less. Symantec DLP Endpoint requires a separate agent on the endpoint in addition to its anti-virus solution. Additional agents slow endpoint performance, translating to more latency and lower productivity. McAfee DLP Endpoint works with McAfee AV as a single agent and can be centrally and automatically deployed and managed by McAfee ePO, leading to easy deployment, management and higher employee productivity.
“RSA excels in scalable data discovery.”	While RSA can scan data at rest, it is unable to index and keep track of data that does not trigger a policy for use with data discovery. RSA requires prior knowledge of sensitive data in order to implement efficient DLP policies. MacAfee's data classification technology address big data issue through rapid data inventory, categorization, and automated remediation.
“RSA offers a comprehensive DLP solution for both network and endpoints.”	RSA continues to have basic endpoint agent. Its clients reported performance and accuracy issues with using some of the advanced content fingerprinting capabilities on the endpoint. McAfee offers flexible and granular DLP policies for both the network and endpoint devices.
“We already have RSA DLP on our endpoints.”	You may have invested in this endpoint solution, but you may not be adequately protected. RSA’s DLP endpoint agent technology offers only basic protection. RSA customers reported performance and accuracy issues with using some of the advanced content fingerprinting capabilities on the endpoint. McAfee DLP Endpoint works with McAfee AV as a single agent and can be centrally and automatically deployed and managed by McAfee ePO, leading to easy deployment, management and higher employee productivity.
“Websense is the industry leader for Web DLP.”	Websense data-in-motion classification is limited to web and email; there is no general network monitoring. It does not have network control for IM protocol, and no network visibility into NNTP traffic, P2P Traffic, telnet traffic, or TCP ports. McAfee offers protection over a much greater range of network protocols.
“Websense is a leader in DLP security. I feel more comfortable recommending and purchasing the recognized leader.”	While Websense has received industry recognition, it recently was acquired by a private equity firm as a result of corporate mismanagement resulting in consistent financial troubles. Since then, the private equity firm Vista, which does not own any other security companies, has enacted a major senior management turnover. Given this acquisition environment, Websense's future is uncertain, and it is unclear how focused they can be now on their products and customers.
“Websense is known to be easy to use. Can McAfee match that?”	Using Websense, the administrator has to create separate policies for data-at-rest and data-in-motion, requiring duplicate efforts. In addition, Websense does not offer discovery for generic HTTP/FTP nor support the scan of Documentum. Websense discovery policies are alerts-only based and without the ability to quarantine. In contrast, McAfee’s DLP solution is easy to use, and can be managed via ePO enabling control alongside other endpoint-related settings.
"We have USB encryption already. Why would we need to buy more?”	What about preventing data-leakage via email? Or web positing? Or printing? Encryption is only a part of a comprehensive data protection. With McAfee DLP, you can secure these other activities as well and benefit from content-aware device control.
"I understand there’s risk, but I’m not certain I’m ready to deploy a DLP solution. I don’t know where to start because I don’t even know where my sensitive data is."	You can deploy McAfee DLP at the pace of your business need, and business readiness, and we offer tools both the tools and services to help you get there. For example, using McAfee’s Capture technology, you instantly gain visibility into where your sensitive data is, how it is being used and who is using it. With this information, you can then take the next step to start incrementally building accurate, targeted DLP policies and deploy and benefit from them faster.