Data Classification for Enterprise Vault Solution Pack

Configured Policies

Notes: By default, all new classification policies are inactive and operate in test mode.

Policy Group	Policy Name	Policy Description
Data_Classification_EV_v11.0	Anti-money laundering	Detects discussions and documents about irregular financial transactions.
	Attorney-Client Privilege	Detects documents and email messages that exhibit the first doctrine of Attorney-Client relations.
	Attorney-Client Privilege (Secondary)	Detects documents and email messages that exhibit the second doctrine of Attorney-Client relations.
	Auto-generated Messages	Detects system replies, such as out of office messages.
	Auto-generated news, feeds, & research (known providers)	Detects messages from known news and research provider email domains.
	Auto-generated news, feeds, research	Detects messages from news providers and feeds using common keywords.
	Compensation Discussions	Detects common keyword identifiers that are found in compensation discussions between employees and human resources or management.
	Email Containers (attachments)	Detects attached email containers.
	Faxes (attachments)	Detects fax attachments.
	Legal Documents (attachments)	Detects legal documents.
	Personal email domains	Detects email that is sent from or sent to known personal email and webmail domains.
	Productivity Documents (attachments)	Detects common office file types.
	Solicitations - Charities	Detects charitable solicitations.
	Solicitations - Political	Detects political solicitations and donations.
	Solicitations -Private Investment	Detects solicitations for venture or private investments.

Available Response Rules

Rule	Action	Conditions
Automated Responses – Classifying Enterprise Vault content		
Classify Enterprise Vault Content (Only available with Enterprise Vault Data Classification Services.)	Classification: Classify Enterprise Vault Content	Execute Always

Saved Reports

Report Name	Description	Filters applied
Events - All	Lists all classification events, sorted by policy, status, and date.	None.
False Positive Events	Lists false positive classification events sorted by policy and date.	Status = False Positive
Positive Events	Lists positive classification events sorted by policy and date.	Status = Positive

Configured Roles and Reports

Role	Description	Reports
Sys Admin	Use this role in place of the built-in Symantec Data Loss Prevention Administrator role. Role Permissions: • User Administration (Superuser) • Server Administration • View (all incidents and classification events) Incident Access: All incidents. Policy Management: No privileges.	None.

Role	Description	Reports

Reporting and Policy Authoring	Use this role for creating and managing all classification policies.
	Role Permissions:
	• View (classification events only)
	• Actions:
	  • Remediate incidents
	  • Look up attributes
	  • Delete incidents
	  • Export Web Archive
	  • XML Export
	  • CSV Attachment in Email Reports
	• Display Attributes (all shared attributes):
	  • Matches
	  • History
	  • Body
	  • Attachments
	  • Sender
	  • Recipients
	  • Subject
	  • Original Message
	• Edit all Custom Attributes
	Incident Access: All incidents.
	Policy Management privileges: Can author policies and response rules, and can access all policy groups.
		None.

Configured Users

User	Role	Description
Admin	Sys Admin (standard system role)	Provides technical system administration for Symantec Data Loss Prevention.
User 1	Reporting and Policy Authoring	Provides ability to create shared reports across other roles without different logins. **Virtual Role—does not need to be assigned to a specific person.**

Attributes Enabled

Status Attributes	Status Group	Status
	Open	New
	Closed	Positive, False Positive

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com