Symantec Data Loss Prevention

Federal Solution Pack

Configured Policies

Policy Group	Policy Name	Policy Description
US Regulatory Enforcement	Defense Message System (DMS) GENSER Classification	This policy detects information classified as confidential according to the guidelines established by the Defense Information Systems Agency for the Defense Message System (DMS) General Services (GENSER) message classifications, categories and markings. These standards outline how to mark classified and sensitive documents according to US standards, as well as providing interoperability with NATO countries and other US allies.
	OMB Memo 06-16 and FIPS 199 Regulations	This policy detects information classified as confidential according to the guidelines established in the Federal Information Processing Standards (FIPS) Publication 199 from the National Institute of Standards and Technology (NIST). These security classifications were reinforced as the basis for compliance with memorandum 06-16 from the Office of Management and Budget (OMB).
Employee Data Protection	Employee Data Protection	This policy detects employee data at risk of exposure.
	US Social Security Numbers	This policy detects patterns indicating Social Security numbers at risk of exposure.
Confidential Data Protection	Confidential Documents	This policy detects company-confidential documents at risk of exposure. (Federal specific keywords added to policy: “Classified, Secret, Top Secret, SBU, Sensitive but Unclassified”)
	Encrypted Data	This policy detects the use of encryption by a variety of methods including S/MIME, PGP, GPG, and file password protection.
	Source Code	This policy detects various types of source code at risk of exposure.
Network Security Enforcement	Network Diagrams	This policy detects computer network diagrams at risk of exposure.
	Network Security	This policy detects evidence of hacking tools and attack planning.
	Password Files	This policy detects password file formats such as SAM, /etc/password, and /etc/shadow.

Available Response Rules

Rule	Action	Conditions
Automated Responses – Blocking Messages		
Block SMTP Email *ONLY available with Network Prevent (Email)*	Block SMTP Message Set Status: Escalated	When Severity Is Any Of High
Block Web Communication *ONLY available with Network Prevent (Web)*	Block HTTP/HTTPS Request Set Status: Escalated	When Protocol is any of HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP And Severity Is Any of High
Remove Web Content *ONLY available with Network Prevent (Web)*	Remove HTTP/HTTPS Web Content Set Status: Escalated	When Protocol is any of HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP And Severity Is Any of High
Automated Responses – Quarantining Emails		
Quarantine SMTP Email *ONLY available with Network Prevent (Email)*	Modify SMTP Message Change Header 1 name to "X-CFilter-Quarantine" and the value to "Yes". Set Status: Escalated	And Severity Is Any of Medium
Automated Responses – Endpoint Actions		
Block Copy to Removable Media *ONLY available with Endpoint Prevent*	Endpoint: Block Set Status: Escalated	When Severity Is Any of High
Notify End User *ONLY available with Endpoint Prevent*	Endpoint: Notify	When Severity Is Any of Medium
Automated Responses – Protecting Files		
Quarantine Stored File (on network file share) *ONLY available with Network Protect*	Protect: Quarantine File Set Status: Escalated	When Severity Is Any of High
Copy Stored File (on network file share) *ONLY available with Network Protect*	Protect: Copy File	When Severity Is Any of Medium
Automated Responses – Resolutions		
Notify and Resolve	Send Email Notification (to sender) Set Status: Resolved Set Resolution Attribute: Automatically Resolved	When Severity Is Any of Low
Resolve with No Action	Set Status: Resolved Set Resolution Attribute: Automatically Resolved	When Severity Is Any of Info
Automated Responses – Notification		
Notify of Critical Incident	Send Email Notification (to manager) Send Email Notification (to sender) Set Status: Escalated	When Severity Is Any of High

Rule	Action	Conditions
Smart Responses - Notifications		
Notify Sender	Send Email Notification (to sender)	Manually Executed
Notify Manager	Send Email Notification (to manager)	Manually Executed
Smart Responses - Escalations		
Escalate for Investigation	Set Status: Investigation	Manually Executed
Smart Responses - Dismissals		
Dismiss, Bus. Process Issue	Set Status: Dismissed Set Dismissal Reason Attribute: Bus. Process Issue	Manually Executed **Strongly recommend adding comment to incident indicating business process and actions to correct**
Dismiss, False Positive	Set Status: Dismissed Set Dismissal Reason Attribute: False Positive	Manually Executed
Smart Responses - Resolutions		
Resolve, Business Issue	Set Status: Resolved Set Resolution Attribute: Business Issue	Manually Executed **Strongly recommend adding comment to incident indicating next steps**
Resolve, Education Issue	Set Status: Resolved Set Resolution Attribute: Education Issue	Manually Executed **Strongly recommend adding comment to incident indicating educational next steps**
Resolve, Employee Oversight	Set Status: Resolved Set Resolution Attribute: Employee Oversight	Manually Executed **Recommend adding comment to incident describing oversight**
Resolve, One-time Event	Set Status: Resolved Set Resolution Attribute: One-time Event	Manually Executed
Resolve, Reply Oversight	Set Status: Resolved Set Resolution Attribute: Reply Oversight	Manually Executed

Configured Roles and Reports

Role	Description	Reports
ISR Access=new status, all policies	InfoSec Responder role. First level of incident response for specific policies. Find broken business processes. Fan-out to extended remediation team. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • No access to sender/recipient identity details • Views or Edits some custom attributes	Incident Queue (for all policies except for HIPAA and Resumes, new status). 1 for each for Network, Endpoint, and Data at Rest.
ISM Access=all statuses; all policies	InfoSec Manager role. Second level of incident response. Manage escalated incidents within InfoSec team. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • Edits all custom attributes • Authors all policies and policy groups • Authors response rules	Incident Queue (for, Competitor Communications, Price, Source Code, Network Diagrams, Network Security, Mergers and Acquisitions, Confidential Documents, Encrypted Data policies, escalated status). 1 for each for Network, Endpoint, and Data at Rest.
Audit Access=all statuses, all policies	Auditor role. Ensure compliance regulations are being met. Develop strategies for risk reduction at Business Unit level. View incident trends and risk scorecards. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • Edits all custom attributes	Incident Queue (for SOX policy). 1 for each for Network, Endpoint, and Data at Rest.

Role	Description	Reports
HRM Access=all statuses, all policies	HR Manager role. HR/Employee Relations Officers. Respond to incidents that lead to employee termination. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • Edits all custom attributes	Incident Queue (for HIPAA and Resume policies, all statuses). 1 for each for Network, Endpoint, and Data at Rest.
Report Access=all statuses, all policies	Reporting and Policy Authoring role. Provides single role for demonstration and Risk Assessment oversight. Role Permissions: • Views incidents/reports • Remediates incidents • No access to incident details • Authors all policies, policy groups, and response rules • No Discover scan control	None
Investigator Access=all statuses, all policies	Researches further details of incidents. Includes incidents forwarded to forensics. Investigates specific employees. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • Edits all custom attributes	Incident Queue (for all policies, Investigation status). 1 for each for Network, Endpoint, and Data at Rest.
Exec Access=all statuses, all policies	Executive role. Ensures data risk reduction at macro level. Reviews risk trends and performance metrics. Reviews risk dashboards. Role Permissions: • Views incidents/reports • Remediates incidents • Looks up attributes • Deletes incidents • Views all custom attributes • No Discover scan control	None

Role	Description	Reports
Sys Admin Access=all statuses, all policies	System Administrator role. To encourage users to use roles other than Administrator. Role Permissions: • User administration • System administration • Views incidents/reports • No access to incident details • No access to shared or custom attributes • No Discover scan control	None

Configured Users

User	Role	Description
Admin	System Admin (standard system role)	Provides technical system administration for Symantec Data Loss Prevention
User 1	All Roles except System Admin	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, Escalated, Investigation
	Closed	Resolved
	Dismissed	Dismissed

Custom Attributes	Resolution*	Dismissal Reason*	Assigned to	Business Unit
	Employee Code	First Name	Last Name	Phone
	Sender Email	Manager Last Name	Manager First Name	Manager Phone
	Manager Email	Region	Country	Postal Code

*The values for these custom attributes should be pre-determined.

Additional Protocols Enabled

Protocols	TCP: Telnet	TCP: SSH	TCP: SSL	TCP: Pop3
	TCP: IRC	TCP: EDonkey	TCP: Gnutella	TCP: BitTorrent
	TCP: Napster	TCP: DirectConnect	TCP: FastTrack	

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com