McAfee Data Loss Prevention Endpoint Proof of Concept

for

Introduction

This document has been prepared to provide a test plan for evaluating McAfee's Data Loss Prevention products to ensure they satisfy the technical requirements of PT XL Axiata Tbk, as described herein. This product is managed and reports to McAfee's central management console, ePolicy Orchestrator (ePO). This document will demonstrate key use-cases, examples of policy management, product deployment, ease-of-use, management, reliability, and customized reporting. This document outlines a testing methodology and success criteria for PT XL Axiata Tbk, based on initial discussions between PT XL Axiata Tbk's information security staff and their McAfee sales representatives and pre-sales engineering staff.

Project Scope and Success Criteria

Most enterprise evaluations require a great deal of time and resources to complete successfully. In order to assist PT XL Axiata Tbk with an effective and thorough evaluation, it is recommended that all success metrics be documented and that weekly update calls/meetings be scheduled between the respective parties to ensure that project timelines are met and any outstanding issues or questions are addressed promptly. Prior to accepting this testing methodology and success definition, please review with McAfee and append any additional success definition that has not been documented prior to starting the Proof of Concept. Once completed, this fully documented set of success definitions will assist in guiding both parties through a successful Proof of Concept in a timely manner. At the conclusion of the testing, PT XL Axiata Tbk will have a sufficient level of understanding of the product to determine if McAfee Data Loss Prevention meets or exceeds expectations to meet PT XL Axiata Tbk's data protection needs.

The primary purpose of installing a Data Loss Prevention solution at PT XL Axiata Tbk is to provide protections against the loss of sensitive information such as regulated data like PCI, PII or PHI and also PT XL Axiata Tbk's Intellectual Property. For the purpose of this evaluation, PT XL Axiata Tbk is most concerned with PCI Regulation.

Evaluating data loss scenarios

The purpose of this guide is to demonstrate McAfee® Data Loss Prevention in action. This guide provides step-by-step instructions to create and test policies that address the following data loss scenarios.

USE CASES

DLP Endpoint

Purpose/Goal	Steps / Description	Success Criteria	Accepted (Y/N)
1. Demontrate DLPe Classification based on file content (Text Patterns)	• Define a text pattern (ie: KTP pattern, NPWP, etc) to be use as an indicator of a confidential file • Set-up a rule to detect and block file which contains those text pattern that were made earlier	McAfee DLPe will detect and block files that contain the defined text pattern from leaving the system	
2. DLPe Classification based on Application	• Define a Tag based on a certain application that frequently used to generate confidential data (ie: internal web application) • Set-up a rule to detect and block the tagged files	McAfee DLPe will detect and block files that generated from the defined application	
3. DLPe Classification based on File Location	• Define a specific location on the network so that everything that is written to that location will be marked/tagged as confidential • Set-up a rule to detect and block the tagged files	McAfee DLPe will detect and block the tagged files	
4. Monitors and blocks Content-Based Copy/Paste action of Confidential file	• Create a Clipboard protection rule from the ePO to block copy/pasting confidential texts to another application • Apply the rule to the client systems • Attempt to copy a portion of text which contains the confidential text pattern and paste it to another application	McAfee DLPe will detect and block user from copying confidential texts	
5. Monitors and blocks confidential files from being posted to the web	• Create a Webpost protection rule from the ePO • Apply the rule to the client systems	McAfee DLPe will detect and block the confidential files from leaving the system through web browser	

Purpose/Goal	Steps / Description	Success Criteria	Accepted (Y/N)
	• Attempt to post confidential files through web browser (ie: sends email through OWA, post comments on social media, upload file to file sharing sites)		
6. Monitors, blocks / encrypts confidential files from being copied to an external drive	• Create a Removable Media Protection rule from the ePO to block copy/pasting confidential file to external drives • Apply the rule to the client systems • Attempt to copy a confidential file to an external drive	McAfee DLPe will detect and block confidential file from being pasted to external drives	
7. Monitors and blocks confidential files from being printed to any printer	• Define a printing protection rule • Apply the rule to the client systems • Attempt to print confidential files to any printer	McAfee DLPe will detect and block confidential file from being printed	
8. Monitors and blocks confidential files from sent via email	Create an email protection rule in the ePO server Apply the rule to the client systems Attempt to send mail through Ms. Outlook	McAfee DLPe will detect and block email containing confidential content from being sent through Ms. Outlook	
9. Monitors and blocks screen capturing of confidential files	Create a Screen Capture rule in the ePO server Apply the rule to the client systems Attempt to capture the screen that haa a tagged file opened	McAfee DLPe will detect and block screen capturing when a tagged file is open	
10. Monitors and blocks confidential files from being copied to cloud	Create a Cloud Protection rule in the ePO Apply it to the client systems Attempt to copy/paste confidential files to the cloud folder	McAfee DLPe will detect and block confidential file from being copied to cloud	

Drive Encryption

Purpose/Goal	Steps / Description	Success Criteria	Accepted (Y/N)
11. Encrypt system's entire disk using McAfee Drive Encryption	• Deploy MDE module to client systems • Assign encryption user and activate MDE	MDE will encrypt disks of the target systems and once MDE is activated, user will be prompted username and password int the preboot authentication page	
12. Resume an on-going encryption process when the system is shut down	• Shut down the system while MDE still encrypting the drives • Turn the system back on	McAfee Drive Encryption will resume the encryption proccess	
13. Recover forgotten password through ePO Administrator	• Create an ePO user which role is to do password recovery • Reboot client systems and choose forgot password • Send the challenge code from client system to ePO Administrator • Input the response code from ePO Adminstrator to the client system	MDE Password can be re-set and user can log in to their system using the new password	
14. Recover forgotten password using smartphone	• Download McAfee Endpoint Assistant application from the app store • save the recovery key to the smrtphone by capturing a QR code from the PBA page	MDE Password can be re-set and user can log in to their system using the new password	
15. Temporarily disable Preboot authentication	• Configure the policy to disable pre-boot authentication • Apply policy to the client system • Reebot the system	PBA page will temporarily disable, the system will boot without the user inputting their MDE username and password	

File and Removable Media Protection

Purpose/Goal	Steps / Description	Success Criteria	Accepted (Y/N)
16. Encrypt entire flash drive	• Configure the FRP policy to enforce encryption to removable drives • Apply the policy to the client systems • Plug a flash drive into the system	McAfee FRP will asks the user to encrypt their flash drive before using them in the system	
17. Let the user define how much space of the flash drive to be encrypted	• Turn on the User-Managed option in the FRP policy • Apply the policy to the client systems • Plug a flash drive into the system	McAfee DLPe will detect and block files that generated from the defined application	
18. Recover forgotten password through ePO Administrator	• Create an ePO user which role is to do password recovery • Plug n encrypted flash drive to the system • Hit the forgot poassword button • Exchange the challenge/response code with the ePO Administrator	FRP password can be re-set and user can log-in to their removable drive using the new password	

CONCLUSION

Results Summary

Criteria	Number	Comments
Use Cases Passed		
Use Cases Failed		

Test Plan Completion Signatures

Exclusive Networks SE Signature

Customer Evaluation Manager Signature

Exclusive Networks SE Name

Customer Evaluation Manager Name

Date

Date