Trellix

DATASHEET

Trellix Data Loss Prevention Endpoint Administration

Education Services Instructor-led Training

The Data Loss Prevention Endpoint Administration course provides in-depth training on the tools you need to design, implement, configure, and use Data Loss Prevention Endpoint to safeguard intellectual property and ensure compliance. The course details how this solution uses ePolicy Orchestrator (ePO) software for centralized management. It also explains how to monitor and address risky, day-to-day end-user actions such as emailing, web posting, printing, clipboards, screen captures, device control, uploading to the cloud, and more.

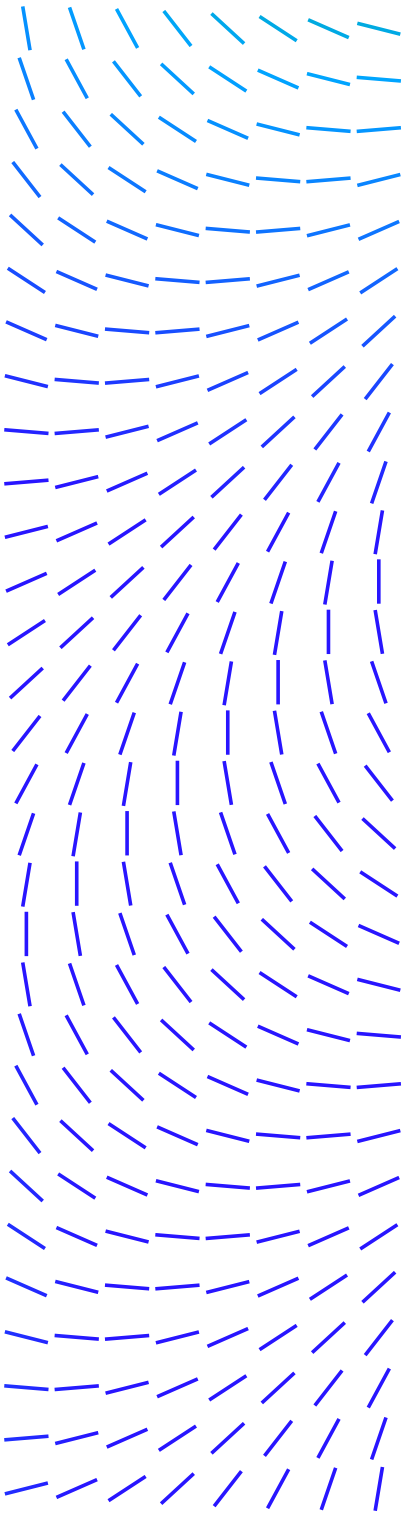
Agenda At A Glance

Day 1

- Welcome
- Data Loss Prevention Solution Overview
- Data Loss Prevention Endpoint Fundamentals
- Planning the Deployment
- Pre-installation system configuration
- Installation
- Deploying client endpoints

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.



Day 2

- Configuring the client
- DLP Help Desk and Permission Sets
- Data Loss Prevention Policy Manager Overview
- Privileged Users and End-User group Definitions
- Device control

Day 3

- Case Studies
- Device rule sets and rules
- Classifying sensitive content
- Content fingerprinting and classification criteria rules
- Data Protection Definitions

Day 4

- Configuring data protection rules
- Endpoint discovery
- Incident Management
- Case Management
- Protecting Files with Rights Management
- File and Removable Media Protection
- Basic Troubleshooting

Learning Objectives

Welcome

Become familiar with information and support resources and feedback mechanisms.

Data Loss Prevention Solution Overview

Describe the solution, its features, and its functionality.

Data Loss Prevention Endpoint Fundamentals

Describe the Data Loss Prevention Endpoint solution, its key features, deployment architecture, and new features and enhancements for this release.

Planning the Deployment

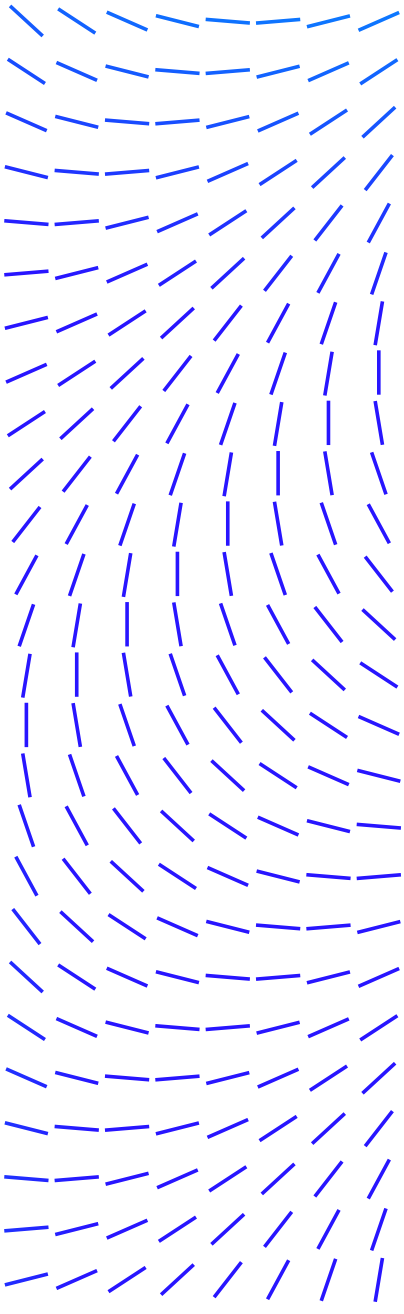
Describe the business, software, hardware, and component requirements to consider when planning deployment.

Pre-Installation System configuration.

Identify the policy design workflow in Data Loss Prevention on MVISION

Recommended Pre-Work

- Solid knowledge of Windows and system administration and network technologies
- Solid knowledge of computer security, cloud security concepts, and web technologies
- Prior experience using McAfee MVISION ePO software



ePO, identify prerequisites for installation, and describe pre-installation tasks.

Installation

Identify the installation process to install or upgrade Data Loss Prevention Endpoint using MVISION ePO. Describe how to configure cloud storage for evidence and fingerprints.

Deploying Client Endpoints

Describe the process to deploy the software to endpoints and verify the success of the deployment.

Configuring the Client

Describe how to configure the Data Loss Prevention Client Configuration Policy and ensure policies are assigned to the appropriate groups or systems.

DLP Help Desk and permission sets

Describe the purpose of the Data Loss Prevention Help Desk and its key features, configure the Help Desk feature, and use the Help Desk feature to generate keys.

Data Loss Prevention Policy Manager Overview

Access the Data Loss Prevention Policy Manager and navigate through Data Loss Prevention Policy Manager tabs to become familiar with its design and use.

Privileged Users and End-User Group Definitions

Register Active Directory server, create a Privileged User, and create End-User group definitions.

Device Control

Describe the Device Control feature, and configure Device Control to meet customer requirements.

Device Rule Sets and Rules

Identify the built-in rule sets and rules available for use, describe the parts of a device rule, and create device rules to meet customer requirements.

Case Studies

Describe how specific rules or classifications would suit a business or industry's needs.

Classifying Sensitive Content

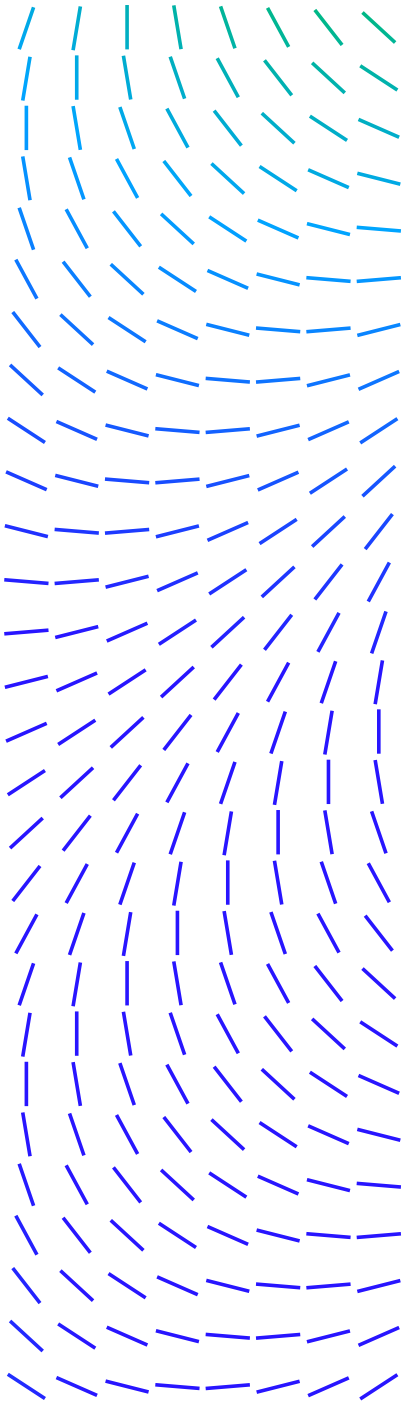
Explain classification definitions and criteria and the Classification module features.

Content Fingerprinting and Classification Criteria Rules

Explain how to create content fingerprinting criteria, how to create

Related Courses

ePolicy Orchestrator Administration



content classification rules, and how persistent fingerprinting works.

Data Protection Definitions

Identify data protection definitions and their associated data protection rules, create definitions used for data protection rules, and configure end-user notifications and justifications.

Configuring Data Protection Rules

Identify the building blocks for data protection, rules, build data protection rules to meet customer requirements, and provide examples of use cases for data protection rules.

Endpoint Discovery

Identify the built-in endpoint discover rules sets and rules available for immediate use, identify the parts of a discovery rule, and create discovery rules to meet customer requirements.

Incident Management

Identify and use the monitoring and reporting features of Data Loss Prevention Endpoint, Including Data Loss Prevention Incident Manager.

Case Management

Describe the functionality of Data Loss Prevention Case Management, create new cases to group related incidents, and administer cases using McAfee Data Loss Prevention Case Management.

Protecting Files with Rights Management

Explain how Rights Management works in the Data Loss Prevention environment, and configure and use supported Right Management products.

Protection Workspace

Describe the functionality of the Protection Workspace in ePolicy Orchestrator.

File and Removable Media Protection

Describe the File and Removable Media Protection solution.

Basic Troubleshooting

Describe the use of the Diagnostic Tool and how to use Debug Logging.