proofpoint.
certified guardian

DATA SHEET

Data Security Administrator for the AI Era

The Data Security Administrator certification course equips system administrators with the expertise to effectively configure, manage, and administer core products within Proofpoint's Data Security platform. These products include Cloud DLP, Endpoint DLP, and Email DLP. This course focuses on key skills such as configuration, customization, and day-to-day management, enabling administrators to defend data and detect risky behavior. This course provides hands-on experience within a classroom-lab environment to hone the data security administrator's skill set and effectively create policies to address common use cases.

Course Syllabus

Platform Overview: In this lesson, you will learn how to:

- Identity the components of Proofpoint's Data Security platform
- Navigate your tenant and system entitlements
- Navigate the Data Security Workbench
- Create, edit, and manage explorations, alerts, and reports
- Create explorations with Advanced Query with AI

User Management: In this module, you will learn how to:

- Configure your Identity Provider
- Add, edit, and assign permissions to user accounts
- Audit console user activities

DATA SECURITY ADMINISTRATOR COURSE

Format:

Virtual Instructor Led Training (VILT), Onsite Training At A Customer's Facilities (OS)

Duration

4

days

Intended Audience:

Data Security Administrators

Data Classification: In this lesson, you will learn how to:

- Identify the purpose and tools of the Data Classification application
- Create effective and efficient data classes and data detectors, including AI classifiers
- Navigate and interact with the Data Security Posture Management Platform (DSPM)
- Create and apply data snippet masking policies

Endpoint Agent Realm Configuration: In this lesson, you will learn how to:

- Explain the features of Endpoint DLP and ITM
- Identify the components of Endpoint/ITM SaaS
- Configure agent realms

Endpoint Agent Deployment: In this lesson, you will learn how to:

- Install agents on endpoints
- Install and configure the agent updater on endpoints

Endpoint Agent Policy Configuration: In this lesson, you will learn how to:

- Identify which features are controlled through agent policies
- Configure effective agent policies
- Assign agent policies to your agent realms

Endpoint and ITM Rules and Conditions: In this lesson, you will learn how to:

- Identify when to use detection, prevention, and endpoint rules
- Create, edit, and apply rules
- Evaluate and fine-tune rules to better fit specific use cases

Endpoint Content Scanning: In this lesson, you will learn how to:

- Identify types of content that can be scanned for sensitive data

Enable content scanning on an agent realm

Email Processes and Policy Routes: In this lesson, you will learn how to:

- Explain the architecture of email services
- Configure email outbound and inbound messages and policy routes

Email Policy Enforcement and Message Investigation: In this lesson, you will learn how to:

- Configure firewall rules and Email DLP rules
- Evaluate and identify when to use Smart Send
- Navigate Smart Search

Cloud Administration, Rule Configuration, and Cloud DLP Rules Configuration and Management: In this module, you will learn how to:

- Configure cloud providers
- Explain access rules, data rules, app governance rules, and configuration and security posture rules
- Configure policies to match specific use cases

Notification Policies: In this module, you will learn how to:

- Identify types of end-user notifications available through Data Security
- Create and apply notification policies
- Create exploration subscriptions

Data Security for AI: In this module, you will learn how to:

- Explain how Data Security for AI can improve visibility into enterprise AI activity
- Monitor and govern shadow AI use
- Identify and protect sensitive data in prompts and uploads