دوره آموزشی Symantec Endpoint Protection Administration

نرم افزار امنیتی **Symantec Endpoint Protection** با بهره گیری از معماری تک **Agent** همراه با ۵ لایه محافظت قوی از مطرح ترین نرم افزارهای امنیتی می باشد. بر اساس آمارها، مدارک بین المللی **Symantec** در رده بالاترین حقوق های دریافتی در دنیا محسوب می شوند. در ایران هم مهمترین شبکه ها و سازمانها شامل وزارتخانه ها، بانک ها، مراکز صنعتی و تجاری، پالایشگاه ها، صنایع نفت و گاز و پتروشیمی، مراکز تحقیقاتی و دانشگاهی و ... بدلیل قدرت و امنیت بالا و قابلیتهای بسیار زیاد از **Symantec Endpoint Protection** استفاده می کنند. نرم افزار **Symantec Endpoint Protection** دارای قابلیتهای وسیعی است و مدیران شبکه و امنیت برای استفاده از این قابلیت ها لازم است به آن تسلط داشته باشند. مرکز آموزش شرکت داده رایانش ابری پردیس با بهره گیری از مجرب ترین اساتید **Symantec** که تجربه پیاده سازی بزرگترین پروژه های آنتی ویروس را در سطح خاورمیانه دارند، دوره های تخصصی **Symantec** را برگزار می کند.

عنوان دوره	مدت دوره	پیش نیاز
Symantec Endpoint Protection Administration	۲۵ ساعت	Network+

Sym\antec Endpoint Protection Administration:

1. Introduction

- Course overview
- The classroom lab environment

2. Symantec Endpoint Protection Product Solution

- Why use Symantec Endpoint Protection?
- Symantec Endpoint Protection technologies
- Symantec Endpoint Protection services
- Symantec Endpoint Protection components
- Symantec Endpoint Protection policies and concepts
- Symantec Endpoint Protection product tiers

3. Installing Symantec Endpoint Protection

- Identifying system requirements
- Preparing servers for installation
- Installing and configuring the Symantec Endpoint Protection Manager
- Describing Symantec Endpoint Protection migration and version compatibility

4. Configuring the Symantec Endpoint Protection Environment

- Starting and navigating the SEPM
- Describing policy types and components
- Console authentication
- Licensing the SEP environment

5. Deploying Clients

- Client requirements and deployment methods
- Preparing for client deployment
- Client installation packages, settings, and features
- Installing managed clients
- Configuring an unmanaged detector
- Upgrading Symantec Endpoint Protection clients

6. Client and Policy Management

- Describing SEPM and client communications
- Administering clients
- Configuring groups
- Configuring locations
- Active Directory integration w ith SEP 12.1
- Client configuration modes
- Configuring domains
- General client settings and Tamper Protection

7. Configuring Content Updates

- Introducing LiveUpdate
- Configuring the SEPM for LiveUpdate
- Configuring the LiveUpdate Settings and Content policies
- Configuring multiple group update providers (GUPs)
- Manually updating virus definitions

8. Designing a Symantec Endpoint Environment

- Architecture and sizing considerations
- Designing the architecture
- Determining client-to-SEPM ratios
- Content distribution methods
- SEPM and database sizing
- Completing the deployment

9. Introducing Antivirus, Insight, and SONAR

- Virus and spyw are protection needs and solutions
- Reputation and Insight
- Administrator-defined scans
- Auto-Protect
- Dow nload Insight
- SONA R
- Included Virus and Spyw are Protection policies

10. Managing Virus and Spyware Protection Policies

- Configuring administrator-defined scans
- Configuring protection technology settings and scans
- Configuring e-mail scans
- Configuring advanced options
- Configuring Mac client detection
- Managing scanned clients
- Configuring Mac Virus and Spyware Protection policy settings

11. Managing Exception Policies

- Exceptions and exclusions
- Configuring the Exceptions policy

12. Introducing Network Threat Protection and Application and Device Control

- Netw ork threat protection basics
- The firew all
- Intrusion prevention
- Application access protection

13. Managing Firewall Policies

- Firew all policy overview
- Defining rule components
- Modifying firew all rules
- Configuring built-in rules
- Configuring protection and stealth settings
- Configuring Windows integration settings

14. Managing Intrusion Prevention Policies

- Configuring intrusion prevention
- Managing custom signatures

15. Managing Application and Device Control Policies

- Creating application and device control policies
- Defining application control
- Modifying policy rules
- Defining device control

16. Customizing Network Threat Protection and Application and Device Control

- Tools for customizing netw ork threat protection
- Managing policy components
- Configuring learned applications
- Configuring system lockdown Virtualization
- Introducing virtualization features
- Virtual image exception
- Shared Insight Cache
- Virtual client tagging
- Offline image scanner

17. Configuring Replication and Failover and Load Balancing

- About sites and replication
- How replication w orks
- Symantec Endpoint Protection replication scenarios
- Configuring replication
- Failover and load balancing

18. Performing Server and Database Management

- Managing SEPM servers
- Maintaining server security
- Communicating w ith other servers
- Managing administrators
- Managing the database
- Disaster recovery techniques