

دوره آموزشی Symantec Endpoint Protection Administration

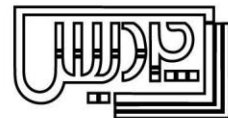
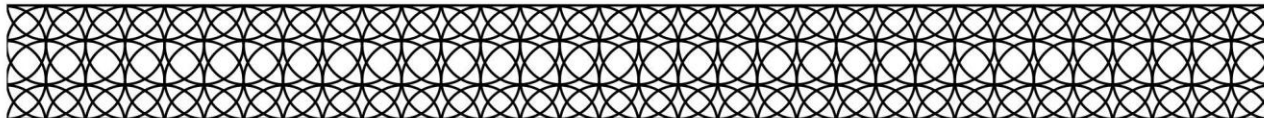
نرم افزار امنیتی **Symantec Endpoint Protection** با بهره گیری از معماری تک **Agent** همراه با ۵ لایه محافظت قوی از مطرح ترین نرم افزارهای امنیتی می باشد. بر اساس آمارها، مدارک بین المللی **Symantec** در رده بالاترین حقوق های دریافتی در دنیا محسوب می شوند. در ایران هم مهمترین شبکه ها و سازمانها شامل 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 قابلیت های بسیار زیاد از **Symantec Endpoint Protection** استفاده می کنند. نرم افزار **Symantec Endpoint Protection** دارای قابلیت های 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.

پیش نیاز	مدت دوره	عنوان دوره
Network+	۲۵ ساعت	Symantec Endpoint Protection Administration
Symantec Endpoint Protection Administration: 1. Introduction <ul style="list-style-type: none"> • Course overview • The classroom lab environment 2. Symantec Endpoint Protection Product Solution <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Starting and navigating the SEPM • Describing policy types and components • Console authentication • Licensing the SEP environment

تهران: میدان ونک - میدان شیخ بهایی - ابتدای خیابان سئول - پلاک ۳۱ - طبقه اول - واحد ۳ - تلفن: ۰۲۱۲۲۱۱۹۸۵۴ - فکس: ۰۲۱۸۹۷۸۳۳۶۷

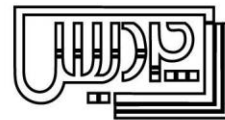
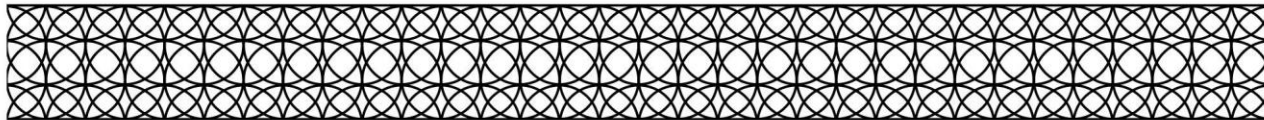
اراک: خیابان امام خمینی (ره) - میدان ولی عصر - جنب لوازم پزشکی کلهر - ساختمان زمرد - واحد ۲۰۴ - تلفن: ۰۸۶۳۲۲۳۵۵۰۴ - فکس: ۰۸۶۳۲۲۱۷۳۲۸





<p>5. Deploying Clients</p> <ul style="list-style-type: none">• 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 <p>6. Client and Policy Management</p> <ul style="list-style-type: none">• Describing SEPM and client communications• Administering clients• Configuring groups• Configuring locations• Active Directory integration with SEP 12.1• Client configuration modes• Configuring domains• General client settings and Tamper Protection <p>7. Configuring Content Updates</p> <ul style="list-style-type: none">• Introducing LiveUpdate• Configuring the SEPM for LiveUpdate• Configuring the LiveUpdate Settings and Content policies• Configuring multiple group update providers (GUPs)• Manually updating virus definitions	<p>8. Designing a Symantec Endpoint Environment</p> <ul style="list-style-type: none">• Architecture and sizing considerations• Designing the architecture• Determining client-to-SEPM ratios• Content distribution methods• SEPM and database sizing• Completing the deployment <p>9. Introducing Antivirus, Insight, and SONAR</p> <ul style="list-style-type: none">• Virus and spyware protection needs and solutions• Reputation and Insight• Administrator-defined scans• Auto-Protect• Download Insight• SONAR• Included Virus and Spyware Protection policies <p>10. Managing Virus and Spyware Protection Policies</p> <ul style="list-style-type: none">• 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
---	---





<p>11. Managing Exception Policies</p> <ul style="list-style-type: none">• Exceptions and exclusions• Configuring the Exceptions policy <p>12. Introducing Network Threat Protection and Application and Device Control</p> <ul style="list-style-type: none">• Network threat protection basics• The firewall• Intrusion prevention• Application access protection <p>13. Managing Firewall Policies</p> <ul style="list-style-type: none">• Firewall policy overview• Defining rule components• Modifying firewall rules• Configuring built-in rules• Configuring protection and stealth settings• Configuring Windows integration settings <p>14. Managing Intrusion Prevention Policies</p> <ul style="list-style-type: none">• Configuring intrusion prevention• Managing custom signatures <p>15. Managing Application and Device Control Policies</p> <ul style="list-style-type: none">• Creating application and device control policies• Defining application control• Modifying policy rules• Defining device control	<p>16. Customizing Network Threat Protection and Application and Device Control</p> <ul style="list-style-type: none">• Tools for customizing network 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 <p>17. Configuring Replication and Failover and Load Balancing</p> <ul style="list-style-type: none">• About sites and replication• How replication works• Symantec Endpoint Protection replication scenarios• Configuring replication• Failover and load balancing <p>18. Performing Server and Database Management</p> <ul style="list-style-type: none">• Managing SEP servers• Maintaining server security• Communicating with other servers• Managing administrators• Managing the database• Disaster recovery techniques
--	---

