

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



NetX delivers both online and onsite instructor-led Symantec and Veritas training courses. Our **high-quality** information security and information management training courses are designed for system administrators, managers, operators, developers, and end users who need to get the job done. Our training classes consist of in-depth presentation and hands-on experience followed by lab access and direct assistance from our **Master Accredited Engineers**.

Attend from your home, office or one of our convenient locations.











Our training classes are **Guaranteed to Run, Symantec classes only!**



NetX training classes are broadcast remotely, allowing our students to attend from any location. *To ensure a positive experience we only allow students to attend remotely and do not mix on-site with remote presentation.*

Smaller classes and 24/5 access are more effective: Each training class has a maximum size of 10 students, ensuring that every participant gets the most out of the presentation and can interface more comfortably with our engineer. 24/5 access to your dedicated training environment allows each student to practice labs as their schedule permits.

Advantages of Training Courses provided by NetX

-  Courses are guaranteed to run because NetX never cancels.
-  Instructors strive to make NetX #1 in customer satisfaction.
-  Instructors are experts with deep, real-world product knowledge.
-  Courses are broadcast online, so you can attend from any location.
-  Virtual training courses conveniently saves time and travel costs.
-  Instructors keep your IT team current and confident.
-  Students gain real-world skills and experience in a hands-on setting.
-  Dedicated labs are available 24 hours a day, 5 days a week.
-  Training Courses have a maximum size of 10 students.
-  Live, instructor-led courses can be held onsite at your location.



Platinum Partner



NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Available Training Courses

Symantec

Symantec/Altiris Asset Management Suite 7.1 Administration course is designed for the asset management professional tasked with installing, configuring, administering, and using Asset Management Suite 7.1 to manage corporate assets in an ITIL-focused environment. SKU: AT1240

Symantec IT Management Suite 8.0 for Administrators course is designed for professionals tasked with using Symantec IT Management Suite (ITMS) to manage their software and hardware resources in their organizations. SKU: 00031871

Symantec/Altiris Deployment Solution 7.5 Administration course is designed for the professional tasked with installing, configuring, and managing a Deployment Solution system. Learn how to simplify the routine tasks of setting up new computers, migrating computers to a new operating system, and moving users to new operating systems or hardware. SKU: AT5997

Symantec Data Loss Prevention 14.6: Administration Symantec Data Loss Prevention 14.x: Administration course is designed to provide you with the fundamental knowledge to configure and administer the Symantec Data Loss Prevention Enforce platform. SKU: SC1409

Symantec Endpoint Protection 14.x Differences course is designed for the network, IT security, and systems administration professionals in a Security Operations position who have experience with SEP 12 and need to understand the new features, how to upgrade to and manage SEP 14. SKU: SC1403

Symantec Endpoint Protection 14.x Manage and Administer course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of the SEPM management console. SKU: SC1404

Symantec Endpoint Protection 14.x Configure and Protect course is designed for the network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14. SKU: SC1412

Symantec Endpoint Protection 14.x Plan and Implement course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with planning and implementing a Symantec Endpoint Protection environment. SKU: 00031681

Symantec Ghost Solution Suite 3.0: Administration course is designed for the professional tasked with installing, configuring, and managing a Deployment Solution system. SKU: SC1420

Symantec Control Compliance Suite 11.0: Administration (3-day) course is designed for professionals who are tasked with ensuring the security of their computing enterprise and compliance with both external and internal mandates. SKU: SC1425

Symantec Control Compliance Suite 11.0: Module Course Options course is designed to enable IT professionals on the additional modules outside the standards manager module which is covered in the CCS 11 Administration Course. SKU: SC1419

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Available Training Courses

Veritas

Veritas Data Insight 5.2: Administration course is designed for the storage administration, IT security, and systems administration professional tasked with architecting, implementing, administering and using Symantec Data Insight. This class covers how to design, install, configure, administer and maintain Symantec Data Insight. SKU: DP0114

Veritas NetBackup 8.0: Administration course provides the IT professional with the general principles, configuration, and management of NetBackup, including how to: best utilize the NetBackup tools and interfaces, effectively monitor backup operations, and ensure data recovery objectives are met. SKU: DP0116

Veritas NetBackup 8.0: Advanced Administration course provides advanced NetBackup topics, including NetBackup performance, disaster recovery, application backups on physical and virtual machines, virtual machine accelerator backups, and security. SKU: DP0115

Veritas NetBackup 8.0: Maintenance and Troubleshooting course provides the IT professional with instruction on troubleshooting NetBackup 7.7 software. This course covers general error detection tools and troubleshooting methodologies. Students practice solving problems related to the NetBackup database, devices, media, disk, deduplication, networking, backups, and restores. In addition, students study the functions of key NetBackup processes and how to enable, view, and manage the associated logs. SKU: DP0113

Veritas Backup Exec 16: Administration course is designed for the data protection professional tasked with architecting, implementing, backing up, and restoring critical data. SKU: DP0117

Veritas NetBackup 2.7.x Appliances: Configuration and Management course provides IT professionals with the skills necessary to configure and manage Symantec NetBackup appliances. SKU: DP0120

Veritas Enterprise Vault 12.x: Implementation and Deployment course is designed for technical support, sales engineers, partners, and customers tasked with providing implementing and deploying the Enterprise Vault 12.x environment. SKU: DP0119

Veritas Enterprise Vault 12.x: Administration 1 course is designed for system administrators tasked with operating, integrating, and monitoring the day-to-day performance of Enterprise Vault within a Microsoft Exchange environment. SKU: DP0127

Veritas Enterprise Vault 12.x: Administration II course is designed for system administrators tasked with operating, integrating, and monitoring the day-to-day performance of Enterprise Vault. SKU: DP0124

Veritas Enterprise Vault 12.x: Administration IIA – Administering File System Archiving course is designed for system administrators tasked with operating, integrating, and monitoring the day-to-day performance of Enterprise Vault. SKU: DP0123

Veritas Enterprise Vault 12.x: Administration IIB – Administering File System Archiving course is designed for system administrators tasked with operating, integrating, and monitoring the day-to-day performance of Enterprise Vault. SKU: DP0122

Veritas Enterprise Vault: DIFFERENCES 11 to 12 course is designed for system administrators tasked with operating, integrating, and monitoring the day-to-day performance of Enterprise Vault within an Exchange environment familiar with Enterprise Vault 11. SKU: DP0131

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Available Training Courses

Veritas (cont.)

Legal Discovery Using Veritas Enterprise Vault 12 Discovery Accelerator course is designed for those who use Discovery Accelerator to search, review, and prepare archived items in support of information requests. SKU: DP0126

Veritas InfoScale 7.2 FUNDAMENTALS for UNIX/Linux: Administration course is designed for the IT professional who wants an overview of the Veritas InfoScale Storage and Veritas InfoScale Availability products. SKU: HA0398

Veritas InfoScale AVAILABILITY 7.2 for UNIX/Linux: Administration course is designed for the IT professional tasked with installing, configuring, and maintaining Veritas Cluster Server (VCS) clusters. SKU: HA0399

Veritas InfoScale STORAGE 7.2 for UNIX/Linux: Administration course is designed for the IT professional tasked with installing, configuring, and maintaining the Veritas InfoScale Storage environments, including Volume Manager (VxVM), File System (VxFS), and Cluster File System (CFS). SKU: HA0401

Veritas eDiscovery Platform 8.2: For Administrators training course is designed for legal professionals that perform Electronic Discovery on Electronically Stored Information. SKU: HA0404

Veritas eDiscovery Platform 8.2: For Users course is designed for legal professionals that perform Electronic Discovery on Electronically Stored Information. SKU: HA0405

Symantec Security Awareness and Compliance Training

Information security demands that employees practice proactive, security-conscious behavior. The Symantec Security Awareness Program trains your employees to understand information security issues and behave in a manner that minimizes risks—all in accordance with current regulatory requirements. The program is designed not only to increase security knowledge and understanding, but also to influence appropriate employee behavior at all levels.

Hosted By NetX

PCI AND HIPAA MODULES

Introduction to HIPAA - HIPAA governs the privacy of an individual's medical records.

Introduction to PCI DSS - PCI DSS is an information security standard which was developed to increase and protect cardholder data during and after a financial transaction.

GENERAL SECURITY AWARENESS MODULES

Passwords - This module teaches efficient new methods of creating and remembering complex passwords required for your organization's security.

How Hackers Get In - It's not rocket science, anymore. Hackers can get in a variety of relatively easy ways – and most of those are through the user. This module reviews the different techniques used.

Human Firewall - This module outlines how users within your organization are a vital part of keeping your organization secure through filtering the information that enters and exits your network.

Privacy - We all enjoy our privacy, and in our modern, digital world, privacy is especially important. This module teaches users what needs to be kept private and how to best protect that privacy.

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Backups - This module outlines what needs to be backed up and how to effectively do that, so that you aren't caught in a bind.

Data Protection and Destruction - This module outlines what data constitutes sensitive data and how to make sure it remains secure before and after you have used it.

Information on the Internet - This module teaches users how information on the Internet can be used against them and how to best protect themselves.

Staying Secure Online - This module outlines how to securely use the Internet so that users can enjoy the resources without exposing themselves to the risks.

Phishing - This module teaches users how to identify different types of phishing attacks.

Appropriate Use - This module outlines how those sites pose a threat to your company's security in order to eliminate a user's willingness to visit those sites while at work.

Insider Threats - This module outlines different ways an organization can be attacked from the inside, as well as how a user can be on the lookout and prevent these types of attacks.

Wi-Fi Security - This module teaches users what to watch out for when connecting to public Wi-Fi, as well as what to avoid doing while connected.

Working Remotely - This module illustrates different practices that should be avoided while working in public to ensure that you and your work are secure.

ROLE BASED TRAINING MODULES

Information Security Risk Management - The module states that four threats or vulnerabilities are in the organization, identifies what the probability and impact those threats are, and analyzes the balance between threats and countermeasures.

Information Security Program Management - This module compares a well-run information security program to a factory, to be set up with a proper plan and well maintained throughout.

Laws and Legality - This module covers the protection of data, personal info, and more. It also covers the Privacy Act, HIPAA, E-Government Law of 2002, and FISMA.

Organization Security Policies - When done right, the policies defined by the information security program determine what is valuable, who should have access to it, how it should be protected, what training is required for different levels of personnel, and what happens when a security issue arises.

System Policies - While federal and program-level policies help establish broad foundational standards, system-specific policies help to ensure the security of computers, networks, applications, and data.

Information Security Program for IT Security - This module focuses on the importance of all the different functions within the security organization.

Contractors - This module explains the importance of screening, documentation, contracts, and more.

CIA Triad - This module explains the importance of remembering these three words, ensuring data and information is kept safe.

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Information Security for Help Desk - The help desk is a crucial part of the information security program in most companies, and as such, should have an extensive understanding of security concepts as well.

IT Architecture Overview - This module explains how to build an IT Architecture and demonstrates how all the parts work together to support one another, such as clouds, firewalls, and networks.

Securing Network Communications - This module focuses on moving data in secure methods, such as encryption and more.

Network Security Controls - This module focuses on network access control to allow only those who are authorized to connect their host to the network.

Information Security Risk Basics - A threat is anything that can harm you or your system. A vulnerability is anything that is considered a weakness in the system. Controls are something that mitigate or deal with threats or vulnerabilities.

System and Data Ownership - This module explains the divide between the IT Department and the business process owners of the data (finance).

Information Security Specific Roles - This module explains the importance of each role within an IT department.

Human Resources Security - The policies and practices implemented should reduce the risk of theft, fraud, or misuse of information by employees, contractors, and third-party users.

Remote Access - This module explains the importance of security of VPN's, USB's, and more. Some of the remote access solutions in the module include limiting the resources that are provided to remote users and strongly enforcing the use of secure authentication mechanisms.

Security in the System Development Lifecycle - Each technology that an organization deploys goes through distinct phases of its deployment. Because of this lifecycle, information security controls need to be integrated at each step to ensure that risk is minimized and each technology runs smoothly. This module focuses on the different steps to make sure this happens.

Operation Security - Information Security needs to take into account how the day-to-day operational activities of this security organization will change to account for a new solution.

The Certification and Accreditation Process - Because of regulations, federal agencies are required to prove that they're doing their jobs protecting information under their control and on their IT Systems. This module explains the process and how this process is designed.

Contracting and System Acquisition - This module explains the risks in the contracting process that should be taken seriously.

Physical Security - This module explains the importance of physical security and keeping the information within your organization safe from a physical standpoint.

Media Handling - A critical component of your organization's security is how your employees handle the data that they are entrusted with. This means they have to manage how they ship, store, destroy, label, and back up media that they use for work purposes.

NetX Training Courses Datasheet

Delivered by Master Accredited Engineers



Contingency Planning and Disaster Recovery - Let's face it, things will go wrong within an organization. But how you plan for the disaster is the difference maker. With a proper plan for the disaster that you face, it can be responded to effectively, and it can be minimized.

User Security - The most important thing to remember is that awareness training is two separate acts. The first goal of what we call "awareness training" is literacy. We put users through this training so they have a common vocabulary about information security. The second step in creating a security-aware user is behavior design. Changing user behavior is often taken for granted.

Improving Information Security Performance through Education - The constant evolution and change within the threat landscape causes the entire industry to constantly change the education landscape. We need to re-engineer security education on a regular basis.

Securing Network Communications - This module focuses on moving data in secure methods, such as encryption and more.

Access Control Basis - Access Control is a collection of methods and components used to protect information assets. It is used to control the confidentiality and integrity of a secure system. It ensures that certain information is available only to those authorized, and those who are not authorized, cannot modify secure information.

Incident Response Basics - While systems are designed to prevent issues from happening, no security control system is 100% effective against attacks. When this happens, a fast and well-practiced response is what allows an organization to limit losses from an incident. The most important factor in quickly responding to successful attacks is to have a well-prepared Computer Security Incident Response Team (CSIRT).

Information Security Program for IT Department - The IT department is in many cases the first responders to a security incident. Because of this, it is a critical piece of the overall Information Security puzzle. IT and InfoSec need to work together as a single unit in order to provide the more secure environment.

Vulnerabilities, Threats, and Controls - When creating an effective IT system, all of the relevant vulnerabilities, threats, and their control measures must be actively observed and considered in order to present the most efficient and secure solution.

Audit and Assessment - The purpose of the Audit and Assessment business unit is to provide an objective, external set of eyes – as a third party – to ensure any IT solution is truly as secure and effective as possible. This module covers those aspects and explains how Audit and Assessment fits into the overall InfoSec posture.

