



**Symantec Enterprise
Product Catalog
October 2005**

SYMANTEC ENTERPRISE SOLUTIONS—OCTOBER 2005

Symantec has developed a new approach to IT management that simultaneously provides for the security and the availability of network resources. Known as Information Integrity™, this balanced approach keeps information safe, yet accessible wherever, whenever, and to whomever business needs dictate. It's an approach designed to help keep businesses up, running, and growing, no matter what happens.

On the following pages, you will find a complete range of world-class enterprise security and availability solutions, including products for preventing intrusions, detecting and removing malicious code, managing enterprise-wide security systems, preserving business continuity, and much more. In short, just about everything you need to ensure the integrity of information assets in your enterprise environment.

Symantec Enterprise Product Catalog

Contents

Appliances	5
Symantec Clientless VPN Gateway 4400 Series	5
Symantec Gateway Security 300 Series	5
Symantec Gateway Security 400 Series	6
Symantec Gateway Security 5400 Series	6
Symantec Gateway Security 5600 Series	7
Symantec Mail Security 8100 Series	7
Symantec Mail Security 8200 Series	8
Symantec Network Security 7100 Series	8
Application Performance Management	9
VERITAS Application Saver	9
VERITAS i3 for ClarifyCRM	9
VERITAS i3 for J2EE	10
VERITAS i3 for .Net	10
VERITAS i3 for Oracle	10
VERITAS i3 for Oracle Applications	11
VERITAS i3 for PeopleSoft	11
VERITAS i3 for SAP	11
VERITAS i3 for Siebel	12
VERITAS i3 for SQL Server	12
VERITAS i3 for Web Servers	12
VERITAS i3 for Web-J2EE	13
VERITAS Indepth for IBM DB2 Universal Database	13
VERITAS Insight Inquire	13
Data Protection	14
VERITAS Backup Exec Project “Panther” Beta	14
VERITAS Backup Exec for NetWare Servers	15
VERITAS Backup Exec for Windows Servers	15
VERITAS Backup Exec for Windows Small Business Server	16
VERITAS Bare Metal Restore	16
VERITAS Enterprise Vault	16
VERITAS NetBackup Enterprise Server	17
VERITAS NetBackup Server	17
VERITAS NetBackup Storage Migrator for UNIX	18
VERITAS Replication Exec	18
VERITAS Storage Exec	18

Contents (cont.)

Early Warning Solutions	19
Symantec DeepSight Alert Services	19
Symantec DeepSight Threat Management System	19
Firewall/VPN	20
Norton Personal Firewall for Macintosh	20
Symantec Clientless VPN Gateway 4400 Series	20
Symantec Enterprise Firewall	21
Symantec Enterprise VPN	21
Symantec Gateway Security 300 Series	21
Symantec Gateway Security 400 Series	22
Symantec Gateway Security 5400 Series	22
High Availability	23
VERITAS Cluster Server	23
VERITAS CommandCentral Availability	23
VERITAS Storage Foundation for Oracle RAC	24
VERITAS Volume Replicator	24
Integrated Security	25
Symantec Client Security	25
Symantec Gateway Security 300 Series	25
Symantec Gateway Security 400 Series	26
Symantec Gateway Security 5400 Series	26
Symantec Gateway Security 5600 Series	26
Intrusion Protection	28
Symantec Decoy Server	28
Symantec Host IDS	28
Symantec Intruder Alert	29
Symantec Network Security	29
Symantec Network Security 7100 Series	29
Security Management	30
Symantec Advanced Manager for Security Gateways	30
Symantec AntiVirus for Handhelds—Corporate Edition with Event and Configuration Manager	30
Symantec Enterprise Security Manager	31
Symantec Event Manager for Intrusion Protection	31
Symantec Event Manager for Security Gateways	31
Symantec Incident Manager	32
Symantec Security Information Manager	32

Contents (cont.)

Storage and Server Automation	33
VERITAS CommandCentral Availability	33
VERITAS CommandCentral Service	33
VERITAS CommandCentral Storage	34
VERITAS OpForce	34
VERITAS Storage Foundation	34
VERITAS Storage Foundation Cluster File System	35
VERITAS Storage Foundation for Databases (DB2, Oracle, and Sybase)	35
VERITAS Storage Foundation for Oracle RAC	35
VERITAS Storage Foundation for Windows	36
Storage and Systems Management	37
STORAGE MANAGEMENT	37
Symantec LiveState Recovery	37
Symantec LiveState Recovery—Restore Anyware Option	38
Symantec LiveState Recovery—LightsOut Restore Option	38
Symantec LiveState Recovery Manager	39
Symantec PartitionMagic Pro	39
Symantec VolumeManager	39
SYSTEMS MANAGEMENT	40
Symantec Discovery	40
Symantec Ghost Solution Suite	40
Symantec LiveState Client Management Suite	41
Symantec LiveState Delivery	41
Symantec LiveState Delivery Enterprise Manager	41
Symantec LiveState Patch Manager	42
Symantec pcAnywhere Corporate Edition	42
Virus Protection, Antispam, and Content Filtering	43
Symantec AntiVirus Enterprise Edition	43
Symantec AntiVirus Corporate Edition	44
Symantec AntiVirus for Caching	44
Symantec AntiVirus for Clearswift	45
Symantec AntiVirus Gateway Solution	45
Symantec AntiVirus for Handhelds—Corporate Edition	46
Symantec AntiVirus for Microsoft Internet Security & Acceleration (ISA) Server 2000	46
Symantec AntiVirus for Microsoft SharePoint	47
Symantec AntiVirus for Network Attached Storage	47
Symantec AntiVirus Scan Engine	47
Symantec Brightmail AntiSpam	48
Symantec Client Security	48
Symantec Client Security for Nokia Communicator	49
Symantec Hosted Mail Security	49

Contents (cont.)

Virus Protection, Antispam, and Content Filtering (cont.)

Symantec Mail Security 8100 Series50
Symantec Mail Security 8200 Series50
Symantec Mail Security for SMTP51
Symantec Mail Security for Domino (for Windows 2000 and Windows Server 2003)51
Symantec Mail Security for Domino Multi-Platform Edition52
Symantec Mail Security for Microsoft Exchange52
Symantec Mobile Security for Symbian53
Symantec Web Security53
Norton AntiVirus for Macintosh54
Norton AntiVirus for Macintosh with Symantec Administration Console for Macintosh54

Vulnerability Management

Symantec NetRecon55
Symantec Vulnerability Assessment55

Symantec Consulting Services

Symantec Advisory Services56
Symantec Solutions Enablement Services56

Symantec Managed Security Services

Early Warning Services57
------------------------------	-----

Appliances: With a family of purpose-built appliances, Symantec makes trusted security easier for any size organization. Symantec plug-and-protect integrated security appliances offer a variety of proven gateway and network protection capabilities—from state-of-the-art firewalls, VPN gateways, and secure remote access, to content filtering, antivirus, Wi-Fi, antispam, and advanced intrusion prevention.

Symantec™ Clientless VPN Gateway 4400 Series



Comprehensive, secure remote access to corporate networks via Web browsers

- Stand-alone, secure remote access appliance (Clientless VPN) that enables remote users to access corporate resources without requiring the installation and maintenance of any client software
- Delivers robust data protection (SSL encryption)
- Extends secure remote access to wireless handheld devices such as Windows Mobile™ 2003 and Palm™ 5 .x-based PDA devices
- Provides portal-based access for Web-enabled and non-Web-based applications via Web VPN
- Enables administrators to configure granular, policy-based user and group extranet access

Symantec™ Gateway Security 300 Series



High-performance, low-maintenance firewall appliance for small businesses

- Powerful firewall protection for the small business network
- Easy-to-manage appliance includes a stateful inspection firewall, secure IPsec VPN connectivity, intrusion detection, intrusion protection, content filtering, and policy enforcement
- Intuitive installation wizard and browser-based management interface simplify setup
- Multifunctional network component that supports LAN switching, Internet sharing, routing, and redundancy
- Optional secure wireless LAN Access Point
- Includes 90 days of support
- Three models (320, 360, 360R) to meet the requirements of organizations from 50–100 nodes

Symantec™ Gateway Security 400 Series



Multifunction firewall appliance provides manageable security for remote and small branch offices

- Integrates stateful inspection firewall with antivirus policy enforcement, IPsec VPN, intrusion detection, intrusion prevention, and content filtering technologies
- Offers integrated networking functions, including a multiport LAN switch, a router, and Internet link protection with automatic detection and failover capabilities
- Provides protection for wireless LAN networks with an Access Point option that extends security protection to clients while allowing seamless roaming within a facility
- Simple installation eases deployment across thousands of remote sites
- Simplifies the task of managing global network security through centralized logging, alerting, reporting, and policy configuration management via a single, Java™-based management console
- Four models meet the needs of any size organization, with a range of supported users, firewall throughput, VPN encryption performance, and load aggregation capabilities

Symantec™ Gateway Security 5400 Series



Full inspection firewall appliance with integrated security technologies

- Seven essential enterprise security functions, which combine firewall protection with protocol anomaly and signature-based intrusion prevention and intrusion detection, award-winning virus protection, URL-based content filtering, antispam, and IPsec-compliant VPN technologies
- Comprehensive network protection to secure networks at the connection to the Internet or subnets of WANs and LANs
- Centralized management simplifies network security management through centralized logging, alerting, reporting, and policy configuration
- Meets the performance requirements of any size organization with an integrated high-availability and load-balancing option
- Three high-performance models deliver throughput scaling from 200 Mbps to more than 3.5 Gbps in a clustered configuration
- Delivers automatic security updates via LiveUpdate™ technology from Symantec™ Security Response, the world's leading Internet security research and support organization

Symantec™ Gateway Security 5600 Series



Easy-to-manage, multifunction security appliances

- Features full-inspection firewall, antivirus protection, intrusion prevention (with antiadware and antispayware capabilities), antispam, intrusion detection, URL-based content filtering with Dynamic Document Review, IPSec, and SSL VPN technologies
- Single console provides comprehensive management of all security technologies to simplify network security management
- Combines multiple detection technologies, including protocol anomaly detection and vulnerability attack interception, to accurately identify and block both known and unknown (or “zero day”) attacks and worms
- Provides component-level redundancy with new hardware platform
- Meets the reliability and performance requirements of any medium enterprise organization offering three high-performance models with scalable throughput and built-in hardware redundancy, plus optional integrated high availability and load balancing
- Delivers automatic security updates via LiveUpdate technology from Symantec Security Response, the world’s leading Internet security research and support organization

Symantec™ Mail Security 8100 Series



Email security appliance that controls spam traffic—stopping spam at the source

- Reduces total email volume up to 50% by stopping spam before it enters the network while ensuring the continuous flow of legitimate mail
- Shapes traffic at the TCP protocol level by prohibiting spammers from forcing mail into a protected network. This causes mail to back up on the spammers’ servers so that their infrastructure rather than yours incurs the burden of spam
- Contains escalating mail infrastructure costs by lowering administrative hardware, storage, and network overhead
- Is easy to install, is compatible with any messaging server, and operates transparently in the network
- Scales to meet the needs of growing businesses. A single appliance handles up to 750,000 user accounts and email loads in excess of 30 million messages a day
- Couple with any antispam gateway solution, including Symantec Mail Security 8200 Series appliances, to provide a comprehensive multilayered approach to combat spam

Symantec™ Mail Security 8200 Series



Email security appliance with integrated, industry-leading antis spam and antivirus technologies

- Powered by industry-leading Symantec Brightmail AntiSpam™ and Symantec AntiVirus™ technologies for effective spam and virus protection
- Appliance form factor and automatic updates enable easy, low-cost deployment and management
- Email firewall technologies reduce email infrastructure costs by restricting connections from spam-sending servers
- Content compliance features allow administrators to gain control over inbound and outbound email content
- All email security appliances can be managed from a single console
- Predefined reports provide insight into trends and attack statistics

Symantec™ Network Security 7100 Series



Proactive intrusion prevention device protects against known and unknown attacks to secure critical networks

- Augments existing gateway and server security deployments to stop threats from propagating throughout networks
- Combines multiple detection technologies, including protocol anomaly detection and vulnerability attack interception, in the IMUNE™ architecture to accurately identify and block both known and unknown attacks and worms
- Helps organizations establish, measure, and report on organizational best practices and compliance initiatives
- Integrated expertise from Symantec Security Response and Services provides early knowledge of threats to enable proactive security
- Requires no network reconfiguration for ease of deployment
- Appliances can support up to eight interfaces*, allowing organizations to monitor more network segments

* Available only with Symantec Network Security 7160 and 7161 models

Application Performance Management: Symantec application service management products optimize the performance and availability of enterprise applications, including popular industry solutions for enterprise resource management (ERP), customer relationship management (CRM), databases, middleware, and more. By integrating application instrumentation, root cause drill-down, and expert advice, Symantec solutions help correct problems in enterprise applications before they can affect business performance.

VERITAS Application Saver (now from Symantec)

Application reliability management

- A comprehensive solution for managing the health of enterprise applications
- Enables first-fault root cause analysis of application failures and offers dynamic fixes to common software defects
- Captures extensive forensics for application faults, including per-thread, statement-level execution histories for both Java and C/C++ applications
- Detects subtle scalability bottlenecks such as excessive lock contentions and virtual memory use
- Helps quickly resolve software defects when applications experience intermittent, inexplicable problems in production environments—before business is impacted

VERITAS i³ for ClarifyCRM (now from Symantec)

Peak performance for ClarifyCRM applications

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning Amdocs ClarifyCRM applications
- Provides a complete view of application performance by capturing, measuring, and correlating performance metrics from each supporting tier of the ClarifyCRM custom applications infrastructure
- Helps detect and pinpoint the cause of problems and identify the most effective course of action to quickly solve the problem and restore systems to peak performance
- Reduces rollout time of ClarifyCRM upgrade projects

VERITAS i³ for J2EE (now from Symantec)

Automatic problem isolation and resolution

- Helps optimize J2EE application performance during the development, testing, and production phases of the application lifecycle—while introducing little to no overhead
 - Provides complete visibility into server-side Java applications, even inside the Java Virtual Machine (JVM™)
 - Maximizes operational efficiency by utilizing SmarTune technology to automate bottleneck detection and correction
 - Helps detect and pinpoint the cause of problems, communicate them to colleagues, and identify the most effective course of action to quickly solve the problem and restore systems to peak performance
-

VERITAS i³ for .Net (now from Symantec)

Complete visibility into .Net production applications

- Delivers performance management to applications utilizing the Microsoft® .Net framework—without introducing additional overhead
 - Provides development, QA, and operational groups with visibility into their .Net applications
 - Helps quickly isolate and resolve performance bottlenecks
 - Makes it easy to share and exchange performance data with colleagues via a browser-based interface
 - Operational dashboards highlight and collate key performance metrics such as top service requests, response time, invocation time, and .Net Performance Counters
-

VERITAS i³ for Oracle (now from Symantec)

Total application and database performance

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning Oracle® environments
- Provides a complete view of application performance by capturing, measuring, and correlating performance metrics from each supporting tier of the Oracle-based custom applications infrastructure
- Helps detect and pinpoint the cause of problems, identify the most effective course of action to quickly solve the problem, and restore systems to peak performance
- Reduces rollout time of Oracle database upgrade projects

VERITAS i³ for Oracle Applications

(now from Symantec)

Peak performance for Oracle applications

- Increases the productivity of Oracle applications end users
 - Reduces rollout time of Oracle E-Business Suite 11i upgrade projects
 - Eliminates the “blamestorming” across technology groups that often accompanies performance slowdowns
 - Finds the definitive root cause of performance degradation in minutes (e.g., Oracle applications users, forms, requests, network, SQL statements, JavaBeans™)
 - Resolves performance problems faster using the expert advice of SmarTune
-

VERITAS i³ for PeopleSoft

(now from Symantec)

Peak performance for PeopleSoft applications

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning PeopleSoft applications
 - Provides a complete view of application performance by capturing, measuring, and correlating performance metrics from each supporting tier of the PeopleSoft applications infrastructure
 - Helps detect and pinpoint the cause of problems, identify the most effective course of action to quickly solve the problem, and restore systems to peak performance
 - Reduces rollout time of PeopleSoft upgrade projects
-

VERITAS i³ for SAP

(now from Symantec)

Peak performance for SAP applications

- Increases the productivity of SAP end users
- Reduces rollout time of SAP upgrade projects
- Eliminates the “blamestorming” across technology groups that often accompanies performance slowdowns
- Finds the definitive root cause of performance degradation in minutes (e.g., t-codes, network, SQL statements, JavaBeans)
- Ensures transaction and application availability via the use of synthetic transactions
- Resolves performance problems faster using the expert advice of SmarTune

VERITAS i³ for Siebel (now from Symantec)

Peak performance for Siebel applications

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning Siebel applications
 - Provides a complete view of application performance by capturing, measuring, and correlating performance metrics from each supporting tier of the Siebel applications infrastructure
 - Helps detect and pinpoint the cause of problems, identify the most effective course of action to quickly solve the problem, and restore systems to peak performance
 - Reduces rollout time of Siebel upgrade projects
-

VERITAS i³ for SQL Server (now from Symantec)

Peak performance for SQL Server–based applications

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning SQL Server environments
 - Provides a complete view of application performance by capturing, measuring, and correlating performance metrics from each supporting tier of the SQL Server–based custom applications infrastructure
 - Helps detect and pinpoint the cause of problems, identify the most effective course of action to quickly solve the problem, and restore systems to peak performance
 - Reduces rollout time of SQL Server upgrade projects
-

VERITAS i³ for Web Servers (now from Symantec)

Peak performance for Web servers

- A comprehensive performance management solution that helps improve end-user response time by proactively monitoring, analyzing, and tuning Web sites and related transactions, and automatically identifying hot spots
- Focuses on the interaction between Web clients and the Web server, helping administrators better manage and measure the performance of business-critical Web-based transactions
- Combines both performance and traffic metrics, helping ensure that service levels are maintained
- Provides complete visibility without introducing overhead, making it ideal for running in production environments and sharing with development, QA, and production groups

VERITAS i³ for Web-J2EE

(now from Symantec)

Peak performance for Web-J2EE applications

- Helps improve end-user response time by proactively monitoring, analyzing, and tuning Web-based applications anchored by J2EE application servers
 - Collects detailed performance data from the Web client, Web server, and J2EE tier, helping users to quickly isolate poorly performing Web pages and transactions, then correlate them with the appropriate J2EE methods
 - Helps detect and pinpoint the cause of problems and identify the most effective course of action to quickly solve the problem and restore systems to peak performance
 - Provides complete visibility into transaction performance without introducing overhead, making it ideal for running in production environments
-

VERITAS Indepth for IBM DB2® Universal Database

(now from Symantec)

Focusing on delivering total application and database performance management

- Generates an accurate, detailed picture of application performance
 - Serves custom-developed, ERP, and e-business applications
 - Delivers rapid, graphical drill-down from the instance level to the root cause
 - Monitors continuously and proactively
 - Provides recent history for diagnosis and resolution after the fact
 - Stores long-term history to support trending and planning
 - Helps improve end-user response time while maximizing the return on technology investment
-

VERITAS Insight Inquire

(now from Symantec)

A proactive approach to application management

- Defines application and transaction performance, availability, and reliability service levels
- Enables IT organizations to take a proactive approach to application availability by allowing critical business transactions and service levels from multiple geographic locations to be profiled and routinely monitored
- Service Level Agreement (SLA) metrics can be easily established and proactively managed, and if service levels are not met or business transaction performance deteriorates, IT staffs are alerted before end users are impacted
- Helps administrators quickly and easily report on key performance metrics such as Mean Time to Repair/Recover (MTTR) and Mean Time Between Failures (MTBF)

Data Protection: The benchmark for data backup and recovery in today's IT environments, Symantec data protection solutions offer scalable protection—from the desktop to the datacenter. Regardless of the type or size of your business, they protect critical data, simplify the management of data backup and recovery, and provide consistent, reliable protection. And as your business grows and requirements change, our scalable products make it easy to cost-effectively upgrade or add options to extend your solution.

VERITAS Backup Exec™ Project “Panther” Beta (now from Symantec)

Delivering true continuous data protection

- Helps ensure that business-critical data is always protected and available through continuous data protection of Windows® servers
- Simplifies data and data restores by enabling end users to retrieve files through a simple, intuitive Web browser without contacting IT
- Helps organizations manage the explosive growth of data by providing faster and more reliable backup and restores using pure disk technology
- Makes retrieving lost, corrupted, or overwritten data as easy as searching for a file from the Internet; no backup tape to locate and load, or data to restore
- Requires no client software or agents installed on the individual desktops and laptops; users only need a standard browser

VERITAS Backup Exec™ for NetWare Servers

(now from Symantec)

Redefining NetWare® data protection

- Novell certified, tested, and approved
 - Delivers faster backup performance by allowing backup and restore from non-removable storage devices, such as hard drives
 - Features an identical graphical user interface from either a NetWare server or a Windows system, delivering complete flexibility to manage a backup environment
 - Provides full protection for the latest Microsoft Windows operating systems via Remote Agent for Windows Servers
 - Multiple slot utility operations and custom label media simplify media administration
 - Duplicate Set Copy enables administrators to copy existing backup sets or those being created during backup to provide redundant backups for offsite storage
-

VERITAS Backup Exec™ for Windows Servers

(now from Symantec)

The gold standard in Windows data protection

- Simplifies and centralizes management and monitoring of multiple VERITAS Backup Exec servers across a distributed network or in remote offices
- Improves manageability of disk-based backups before moving them onto tape, supporting disk-to-disk-to-tape backup and restore strategies
- Enables fastest backups and restores through advanced disk-based backup and recovery, including Synthetic and Off-Host backups to perform near zero impact backups and fast restores
- Provides high-performance, network-wide data protection for 32- and 64-bit remote Linux® and UNIX servers
- Safeguards SharePoint® Portal Server 2001 and 2003 with online, fast, and reliable data protection and granular recovery
- Integrates VERITAS Replication Exec and VERITAS Storage Exec functionality via SmartLink technology for improved centralized administration

VERITAS Backup Exec™ for Windows Small Business Server (now from Symantec)

Leading Windows data protection solution for small businesses

- Complements Microsoft Windows Small Business Server Editions to provide an end-to-end foundation for networking and complete data protection
 - Delivers cost-effective, easy-to-use, and highly reliable data protection, plus fast backup and restore of applications
 - Features backup, restore, disaster recovery, single-drive library support, Exchange Server, SQL Server, and SharePoint Services protection and recovery
 - Includes powerful agents and options to deliver robust storage management tools to meet diverse application needs for growing and upgrading storage
-

VERITAS Bare Metal Restore™ (now from Symantec)

Simplifying and automating server recovery

- Automates and streamlines the server recovery process, making it unnecessary to manually reinstall operating systems or configure hardware
 - Complete server restores can be accomplished in a fraction of the time with simple commands, and without extensive training or tedious administration
 - Enables administrators to execute multiple server restores in parallel to accomplish mass-recovery operations—all from a browser-based, wizard-driven interface
 - Addresses the demands of multiple platforms, eliminating the need for customized restore procedures on each platform
 - Enhances the availability of critical data, helping administrators deliver IT as a utility
-

VERITAS Enterprise Vault™ (now from Symantec)

Store, manage, protect, and discover business information

- Provides a flexible archiving framework to enable the discovery of content held within email, file system, and collaborative environments, while helping to reduce storage costs and simplifying management
- Manages content via automated, policy-controlled archiving to online stores for active retention and seamless retrieval of information
- Complemented by specialized client applications for enhancing corporate governance, risk management, and legal protection
- Helps organizations reduce business and IT risks surrounding application storage management; compliance retention and discovery; and upgrade, migration, and consolidation

VERITAS NetBackup™ Enterprise Server

(now from Symantec)

Complete data protection for the most complex UNIX, Windows, Linux, and NetWare environments

- Synthetic backup method delivers quick client restore from a single backup image
 - Leverages high-performance disk as a cache prior to storing backup data on long-term storage, helping reap the benefits of both tape and disk media
 - Centralized management and control, high-performance technology, and a flexible multi-tier architecture scale to meet the growing needs of the modern datacenter
 - Supports 64-bit platforms and databases, helping protect all major UNIX variants, Windows, Linux, and NetWare systems
 - Low-impact encryption option ensures that data is secure before it leaves the client
 - Supports a broad range of tape library, tape drive, and storage area network (SAN) interconnect technologies from leading vendors
-

VERITAS NetBackup™ Server

(now from Symantec)

Innovative data protection

- Delivers end-to-end data protection for all environments from desktop to datacenter to vault
- Helps consolidate and standardize backup and recovery operations, protecting all major UNIX variants, Windows, Linux, and NetWare systems
- Consumes less network bandwidth and decreases the impact on the application host since files are backed up only once
- Multiplexing up to 32 different data streams to a single tape drive helps to realize the maximum rated throughput of storage hardware
- Allows users to share an automated tape library between heterogeneous systems, enabling users to more effectively leverage expensive tape and drive resources
- Secures backup data with a variety of encryption options
- Supports a broad range of tape library and tape drive interconnect technologies from leading vendors

VERITAS NetBackup™ Storage Migrator for UNIX (now from Symantec)

Automated data lifecycle management

- Extends NetBackup by integrating with the NetBackup media manager to migrate data from online storage to backup media
 - Migrating Oracle Archive/Redo logs allows users to store more logs for easier point-in-time recovery of Oracle databases
 - Streamlines data protection and disaster recovery—in the event of a restore, the system needs to recover only a placeholder, not the entire file, while multiple copies of migrated data can be created for greater disaster protection
 - Enables managers to configure policies to meet their unique data life cycles in a consistent, automated, cost-effective manner
 - Integrates with NetBackup for offline or nearline media management, as well as for sharing existing tape libraries
-

VERITAS Replication Exec™ (now from Symantec)

Continuous protection for remote offices

- Uses real-time replication to copy data from remote servers to a central server
 - Powerful administrator console can be managed from a single location
 - Easy-to-use interface has the same look-and-feel as VERITAS Backup Exec
 - Automated technology ensures remote office data protection with minimal administration
 - Replicates data continuously or on a scheduled basis
 - Efficiently replicates only changed data in 64 KB blocks
-

VERITAS Storage Exec™ (now from Symantec)

Superior Windows data management

- Integrates with VERITAS Backup Exec to deliver simple, automated data management and faster backup times
- Gives administrators the power to identify and recover wasted disk space, create and enforce policies to limit user disk space, and block unwanted file types from business servers
- Provides detailed reports to discover problem areas
- Helps reduce storage growth and limit legal exposure

Early Warning Solutions: Your enterprise is constantly reacting to new threats and vulnerabilities. To provide reassurance in risky enterprise environments, Symantec offers customized early warning alerts of cyberattacks, along with threat analysis and countermeasures to prevent attacks before they occur. Symantec early warning solutions enable companies worldwide to mitigate risk, manage threats, and ensure business continuity.

Symantec DeepSight™ Alert Services

Helping to proactively ensure business continuity through the timely delivery of actionable security information

- Monitors vulnerabilities in more than 18,000 technologies, from 2,200 vendors, and automatically delivers timely security notifications worldwide
- Optional XML output for integration into IT security processes and remediation solutions, such as Remedy Help Desk, and enables tracking of actions by the security and IT team
- Alert status tracking streamlines task assignment and reporting by providing status and documenting resolutions
- Provides analysis and guidance on how to mitigate risks by using technologies such as IDS or firewall, even before virus definition files are available
- Personalization enables security resources to receive only alerts relevant to their enterprise environment and their specific areas of responsibility
- Offers a range of delivery options, including email, voice, fax, and SMS

Symantec DeepSight™ Threat Management System

Helping to protect networks from active threats with an industry-leading, Web-based early warning security system

- Detailed alerts provide timely intelligence on security incidents aggregated from thousands of exclusive sources and attack sensors worldwide
- Actionable intelligence enables more efficient prioritization, allocation, and deployment of security staff and resources
- Complete personalization allows administrators to configure automated alerts and reports for the requirements of their unique IT infrastructure
- Powerful tracking and reporting capabilities help quantify security ROI for resource allocation and expense justification ranging from time period to industry type to attack specifics
- Backed by Symantec Security Response, the world's leading Internet security research and support organization

Firewall/VPN: Symantec's comprehensive firewall and VPN family makes it easy for organizations of any size—from single offices to global enterprises—to connect securely with customers, partners, and remote users. The family of firewall/VPN solutions offers enterprise-class protection and the highest levels of certification, as well as integrated, all-in-one solutions that, in addition to ensuring secure access to enterprise resources, provide critical protection against viruses, spyware, intrusions, and more.

Norton™ Personal Firewall for Macintosh®

Keeps hackers out and personal data in

- Automated setup eases installation
- Allows administrators to control outbound as well as inbound connections to defend against spyware and Trojan horses
- Detects all available Internet services and only activates them upon user request
- One-click setting allows administrators to limit access to a computer, or to users on the LAN or Internet
- Allows user to turn off the Rendezvous™ service on a Mac® system
- Displays a list of all currently connected users

Symantec™ Clientless VPN Gateway 4400 Series



Comprehensive, secure remote access to corporate networks via Web browsers

- Stand-alone, secure remote access appliance (Clientless VPN) that enables remote users to access corporate resources without requiring the installation and maintenance of any client software
- Delivers robust data protection (SSL encryption)
- Extends secure remote access to wireless handheld devices such as Windows Mobile 2003 and Palm 5 .x-based PDA devices
- Provides portal-based access for Web-enabled and non-Web-based applications via Web VPN
- Enables administrators to configure granular, policy-based user and group extranet access

Symantec™ Enterprise Firewall

Fast and secure application-level protection against unwanted network intrusion

- Provides proactive security and protects the network against blended threats by default
 - Full Application Inspection technology enables the inspection of data deep inside packets passing through the security gateway, providing enterprise-class protection for both application- and network-level attacks
 - Centralized management simplifies managing network security through centralized logging, alerting, reporting, and policy configuration
 - Meets performance requirements with an integrated high-availability and load-balancing option
 - Extensive platform support for Windows and Solaris™
-

Symantec™ Enterprise VPN

A secure and easy-to-manage virtual private network

- Supports a 50-user license tier
 - Ensures maximum security and performance by supporting the Advanced Encryption Standard (AES) algorithm
 - Remote policies create a boot strap file for the client
 - Interoperability with Symantec™ Firewall/VPN appliance models 100, 200, and 200R
 - Support for Windows XP for Symantec Enterprise VPN Client
 - Establishes secure, fast, and inexpensive links between corporate offices, mobile users, and business partners
-

Symantec™ Gateway Security 300 Series



High-performance, low-maintenance firewall appliance for small businesses

- Powerful firewall protection for the small business network
- Easy-to-manage appliance includes a stateful inspection firewall, secure IPsec VPN connectivity, intrusion detection, intrusion protection, content filtering, and policy enforcement
- Intuitive installation wizard and browser-based management interface simplify setup
- Multifunctional network component that supports LAN switching, Internet sharing, routing, and redundancy
- Optional secure wireless LAN Access Point
- Includes 90 days of support

Symantec™ Gateway Security 400 Series



Multifunction firewall appliance provides manageable security for remote and small branch offices

- Integrates stateful inspection firewall with antivirus policy enforcement, IPsec VPN, intrusion detection, intrusion prevention, and content filtering technologies
- Offers integrated networking functions, including a multiport LAN switch, a router, and Internet link protection with automatic detection and failover capabilities
- Provides protection for wireless LAN networks with an Access Point option that extends security protection to clients while allowing seamless roaming within a facility
- Simple installation eases deployment across thousands of remote sites
- Simplifies the task of managing global network security through centralized logging, alerting, reporting, and policy configuration management via a single, Java-based management console
- Four models meet the needs of any size organization, with a range of supported users, firewall throughput, VPN encryption performance, and load aggregation capabilities

Symantec™ Gateway Security 5400 Series



Full inspection firewall appliance with integrated security technologies

- Seven essential enterprise security functions, which combine firewall protection with protocol anomaly and signature-based intrusion prevention and intrusion detection, award-winning virus protection, URL-based content filtering, antispam, and IPsec-compliant VPN technologies
- Comprehensive network protection to secure networks at the connection to the Internet or subnets of WANs and LANs
- Centralized management simplifies managing network security through centralized logging, alerting, reporting, and policy configuration
- Meets the performance requirements of any size organization with an integrated high-availability and load-balancing option
- Three high-performance models deliver throughput scaling from 200 Mbps to more than 3.5 Gbps in a clustered configuration
- Delivers automatic security updates via LiveUpdate technology from Symantec Security Response, the world's leading Internet security research and support organization

High Availability: Every day, IT faces the challenge of providing high levels of data and application availability across a wide array of operating systems, applications, hardware components, and datacenter locations. Even in the most diverse environments, organizations can be assured that Symantec clustering and replication solutions will deliver the ultimate in high availability for data and applications.

VERITAS Cluster Server™ (now from Symantec)

Powerful protection against application and database downtime

- The industry's leading open systems clustering solution to protect critical applications, data, and databases from downtime
- Helps maximize uptime and reduce both planned and unplanned downtime
- Enables high availability for local, metropolitan, or global clustering from within a single product
- Allows administrators to test disaster recovery solutions without impacting production applications or resources
- Portable modeling and simulation tool helps optimize and plan cluster configuration and policies
- Provides investment protection by using the same clustering tool across all open systems and improves hardware utilization by intelligently moving applications to available servers

VERITAS CommandCentral™ Availability (now from Symantec)

Application availability management for the enterprise

- Improves application availability while increasing administrator efficiency
- Facilitates the management of clustered servers by ensuring that clusters are configured correctly
- Helps find and prevent human errors, and identifies failures based on historical data to avoid repeating mistakes
- Automates cluster operations so administrators can resolve problems faster and devote more time to areas that affect the bottom line

VERITAS Storage Foundation™ for Oracle RAC (now from Symantec)

The most manageable RAC solution in the industry

- Provides an integrated solution optimized for Oracle Real Application Clusters
 - Includes Cluster File System, Cluster Volume Manager, and Cluster Server to help implement robust, manageable, and scalable Oracle RAC
 - Delivers the industry's first heterogeneous cluster file system supporting Oracle RAC on the Solaris, Linux, AIX, and HP-UX operating systems
 - Dramatically simplifies the installation and ongoing management costs of an Oracle RAC environment
 - Gives administrators the flexibility to create clustering solutions using best-of-breed storage hardware, allowing organizations to adapt to their changing technology requirements and contain costs
-

VERITAS Volume Replicator™ (now from Symantec)

Enterprise-class disaster recovery for mission-critical environments

- Performs comprehensive volume group replication in both synchronous and asynchronous modes to ensure data integrity and consistency
- Scales to support up to 32 secondary replication sites for many-to-one or one-to-many scenarios
- Intuitive Web- and Java-based consoles assist with configuration, monitoring, and online administration
- Integrates with Cluster Server and the Global Cluster Option to allow for the monitoring of replication across sites and ensure that replication services are highly available
- Fully supports most commercial database management systems, including SQL Server and Exchange
- Replicates between all major hardware platforms to eliminate vendor-specific storage limitations

Integrated Security: As IT organizations are tasked to secure increasingly sophisticated environments, demand is growing for solutions that are easier to use and less expensive to maintain. With that in mind, Symantec pioneered integrated security. Symantec's scalable integrated security products combine firewall, intrusion prevention, antivirus, and other client and gateway security technologies, and set a new standard with protection that is more secure, less expensive, and easier to manage.

Symantec™ Client Security

Proactively protects against blended threats through robust client protection, centralized management, and ease of administration

- Integrated security technologies proactively protect enterprise client systems from security risks and network intrusions
- NEW! Generic Exploit Blocking enhances intrusion prevention capabilities, resulting in reduced time-to-protection after vulnerability announcements
- NEW! Optimized out-of-the-box firewall configurations minimize configuration efforts while stopping the majority of threats
- Backed by Symantec Security Response, the world's leading Internet security research and support organization
- NEW! Enhanced protection from spyware and adware, including:
 - Real-time protection to reduce the risk of spyware reaching the system
 - Automatic removal for easy disposal of security risks
 - Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find spyware infection
 - Control over spyware settings via existing Symantec™ AntiVirus Corporate Edition management interface

Symantec™ Gateway Security 300 Series



High-performance, low-maintenance firewall appliance for small businesses

- Powerful firewall protection for the small business network
- Easy-to-manage appliance includes a stateful inspection firewall, secure IPsec VPN connectivity, intrusion detection, intrusion protection, content filtering, and policy enforcement
- Intuitive installation wizard and browser-based management interface simplify setup
- Multifunctional network component that supports LAN switching, Internet sharing, routing, and redundancy
- Optional secure wireless LAN Access Point
- Includes 90 days of support

Symantec™ Gateway Security 400 Series



Multifunction firewall appliance provides manageable security for remote and small branch offices

- Integrates stateful inspection firewall with antivirus policy enforcement, IPsec VPN, intrusion detection, intrusion prevention, and content filtering technologies
- Offers integrated networking functions, including a multiport LAN switch, a router, and Internet link protection with automatic detection and failover capabilities
- Provides protection for wireless LAN networks with an Access Point option that extends security protection to clients while allowing seamless roaming within a facility
- Simple installation eases deployment across thousands of remote sites
- Simplifies the task of managing global network security through centralized logging, alerting, reporting, and policy configuration management via a single, Java-based management console
- Four models meet the needs of any size organization, with a range of supported users, firewall throughput, VPN encryption performance, and load aggregation capabilities

Symantec™ Gateway Security 5400 Series



Full inspection firewall appliance with integrated security technologies

- Seven essential enterprise security functions, which combine firewall protection with protocol anomaly and signature-based intrusion prevention and intrusion detection, award-winning virus protection, URL-based content filtering, antispam, and IPsec-compliant VPN technologies
- Comprehensive network protection to secure networks at the connection to the Internet or subnets of WANs and LANs
- Centralized management simplifies managing network security through centralized logging, alerting, reporting, and policy configuration
- Meets the performance requirements of any size organization with an integrated high-availability and load-balancing option
- Three high-performance models deliver throughput scaling from 200 Mbps to more than 3.5 Gbps in a clustered configuration
- Delivers automatic security updates via LiveUpdate technology from Symantec Security Response, the world's leading Internet security research and support organization

Symantec™ Gateway Security 5600 Series



Easy-to-manage, multifunction security appliances

- Features full-inspection firewall, antivirus protection, intrusion prevention (with antiadware and antispyware capabilities), antispam, intrusion detection, URL-based content filtering with Dynamic Document Review, IPSec, and SSL VPN technologies
- Single console provides comprehensive management of all security technologies to simplify network security management
- Combines multiple detection technologies, including protocol anomaly detection and vulnerability attack interception, to accurately identify and block both known and unknown (or “zero day”) attacks and worms
- Provides component-level redundancy with new hardware platform
- Meets the reliability and performance requirements of any medium enterprise organization offering three high-performance models with scalable throughput and built-in hardware redundancy, plus optional integrated high availability and load balancing
- Delivers automatic security updates via LiveUpdate technology from Symantec Security Response, the world’s leading Internet security research and support organization

Intrusion Protection: Symantec intrusion protection solutions fortify an organization's overall security posture, allowing it to securely leverage all the benefits the Internet offers. Utilizing a multilayered, proactive approach, they monitor traffic, detect breaches, and respond to attacks in real time. And with flexible administration that helps control costs and enforce security policies, they make it easy to identify and prevent inappropriate activities from occurring on networks and host systems.

Symantec™ Decoy Server

Early detection solution for cost-effective threat prioritization

- Detects unauthorized access and system misuse to provide enterprises with cost-effective prioritization of threats
- Improved ability to create simulated email traffic between users to enhance the decoy environment
- Improved response mechanisms include frequency-based policies and the ability to shut down systems based on attacker activity
- Improved reporting and logging capabilities ease report creation and enhance prioritization efforts and incident resolution
- Provides early detection and early warning of threats, supplying information crucial to maintaining a productive network infrastructure
- Enables stealth monitoring and containment plus live attack analysis

Symantec™ Host IDS

Intrusion detection and prevention technology with advanced management capabilities

- Monitors systems in real time to detect and respond to security breaches and other unauthorized activities
- Process management capabilities combine multiple intrusion prevention technology functions to allow organizations to respond rapidly to intrusions and make informed security policy decisions to protect critical servers
- Enables the creation of customizable host-based intrusion detection policies and responses
- Centralized management tools simplify the monitoring and enforcement of host intrusion detection security policies
- Integrates with the Symantec™ Security Management System to deliver enhanced prioritization, identification, containment, and removal of security threats
- Provides audit data for incident and forensic analysis, and generates graphical reports of intrusion activity

Symantec Intruder Alert™

Host-based intrusion detection and security policy management

- Monitors user actions continuously to detect and prevent unauthorized activity
 - Provides powerful intrusion detection system (IDS) policy creation and customization
 - Ensures that current policies are enforced with the immediate deployment of new or modified IDS policies and signatures
 - Illustrates activity in concise tables and graphs for both host and network IDS activity
 - Collects and securely preserves audit data for archival and post-event analysis
 - Allows administrators to manage network-wide responses from a single console
-

Symantec™ Network Security

(formerly known as Symantec ManHunt™)

High-speed, advanced network intrusion detection software solution

- Augments existing gateway and server security deployments to stop threats from propagating throughout networks
 - Combines multiple detection technologies, including protocol anomaly detection and vulnerability attack interception, in the IMMUNE architecture to accurately identify and block both known and zero-day attacks and worms
 - Requires no network reconfiguration for ease of deployment
 - Three models support aggregate network bandwidth from 50 MBps to 2 GBps to meet deployment needs at branch offices, distribution sites, and the network core
 - AutoProtect automatically updates protection policies using LiveUpdate technology to help organizations stay ahead of continuously evolving threats
 - One-Click to Prevention transitions the appliance from a detection device to a prevention tool with a single mouse click
-

Symantec™ Network Security 7100 Series

Proactive intrusion prevention device protects against known and unknown attacks to secure critical networks

- Augments existing gateway and server security deployments to stop threats from propagating throughout networks
- Combines multiple detection technologies, including protocol anomaly detection and vulnerability attack interception, in the IMMUNE architecture to accurately identify and block both known and unknown attacks and worms
- Helps organizations establish, measure, and report on organizational best practices and compliance initiatives
- Integrated expertise from Symantec Security Response and Services provides early knowledge of threats to enable proactive security
- Requires no network reconfiguration for ease of deployment
- Appliances can support up to eight interfaces*, allowing organizations to monitor more network segments

* Available only with Symantec Network Security 7160 and 7161 models

Security Management: Symantec security management solutions provide a 360° view into an enterprise's risk exposure, enabling organizations to confidently take action in times of crisis to contain security threats. They extend across multiple platforms and security products, including firewalls, intrusion protection, and antivirus software. By consolidating security event data and analyzing risks and vulnerabilities proactively, they provide actionable intelligence that promotes the development of better security policies and compliance, plus a stronger overall security posture.

Symantec Advanced Manager for Security Gateways

Enables a wide range of advanced management and reporting capabilities via a centralized, Web-based management console

- Transforms enterprise-wide security event data into useful and actionable security information
 - Builds IT credibility and enables better decision-making with centralized, consolidated information and insightful analyses
 - Delivers a complete view of an enterprise's security posture and enables proactive identification of vulnerabilities
 - Provides secure, centralized, Web-based management of hundreds or thousands of Symantec security gateway products across the enterprise
-

Symantec AntiVirus™ for Handhelds—Corporate Edition with Event and Configuration Manager

(available for U.S. customers only)

Comprehensive, reliable protection for Palm OS® and Pocket PC handheld devices

- Provides centralized control with configuration, implementation, and enforcement of policies from a single console
- Event and configuration console can be used to view multiple security products
- Enables logging, alerting, and reporting information to be managed through a centralized management console
- Administration and configuration allows administrators to manage local and remote devices, and configure and enforce security policies over the Internet
- Common alerting, logging, and reporting for custom analysis and session trends
- Management console provides an integrated view of multiple security products, as well as the status of the network

Symantec Enterprise Security Manager™

Demonstrate compliance with security policies and government regulations

- Provides more than 3,000 specific security checks to help ensure that mission-critical information systems comply with an organization's security policies
 - Includes new policy assessment templates and research for regulations such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act, as well as updates for HIPAA, NERC, and FISMA (NIST 800-53) regulations and SANS Top 20 and ISO 17799 industry standards
 - Delivers flexible and powerful enterprise-class compliance reporting, including 75 predefined reports, as well as ad hoc reports using the advanced report-authoring tool
 - Reports for business management include overall compliance levels, resolution, and enterprise-wide trends
 - Reports for technical managers detail compliance at the system, operating system, or line-of-business level
 - Integrates with other Symantec™ Security Management System products to enable a more holistic understanding of security risks and priorities
-

Symantec™ Event Manager for Intrusion Protection

Centralized monitoring, alerting, and reporting for Symantec and select third-party intrusion protection and intrusion prevention solutions

- Provides a holistic, centralized view of Symantec and select third-party intrusion protection and intrusion prevention deployments across all network tiers
 - Minimizes management costs and complexity with centralized, multilayered monitoring, alerting, and reporting of intrusion events
 - Delivers enterprise-level reporting for all supported intrusion protection products
 - Enhances IT credibility and enables better decision-making with centralized, consolidated information and insightful analyses
 - Helps improve security posture enterprise-wide
-

Symantec™ Event Manager for Security Gateways

Centralized logging, alerting, and reporting across Symantec's security gateway protection solutions and select third-party products

- Provides a consistent, holistic view of Symantec's security gateway protection solutions and select third-party gateway solutions, helping to improve security posture enterprise-wide
- Minimizes management costs and complexity with centralized logging, alerting, and reporting
- Transforms event data from security gateway deployments across the enterprise into actionable security information, helping to reduce information clutter
- Maximizes the system uptime by accelerating response time to security incidents and blended security threats
- Enhances IT credibility and enables better decision-making with centralized, consolidated information and insightful analyses
- Offers optional third-party security gateway solutions and network management systems from leading vendors

Symantec™ Incident Manager

Real-time security incident management for enterprise network environments

- Powerful, automated, near-real-time correlation engine transforms security data into actionable intelligence, enabling rapid response to complex security threats
- Accurately detects and identifies attacks while reducing monitoring costs
- Tracks incident handling activities from identification to closure, keeping the focus on corrective action
- Optional bidirectional communication with Remedy® Help Desk* ensures coordination remediation between IT and security teams

* Available at additional cost

Symantec™ Security Information Manager

Next-generation real-time security information management appliances for enterprise network environments

- Proactively protects and responds to global threats through continuous dynamic correlation of Symantec's Global Security Intelligence
- Enables automatic identification and prioritization of security threats that impact business-critical applications
- Links helpdesk IT operations workflow processes to ensure compliance to corporate security policies
- Reduces deployment and maintenance complexities and enables greater staff efficiencies
- High-performing, extensible, and scalable appliances that are easy to deploy, easy to use, and easy to maintain
- Optional bidirectional communication with Remedy® Help Desk* and Perregrine ServiceDesk ensures coordination remediation between IT and security teams

* Available at additional cost

Storage and Server Automation: Symantec automation products lead the market in interoperable solutions that work seamlessly across heterogeneous environments to manage IT resources. They help organizations reduce complexity, maintain continuous application availability, and provide services that are measurable, accountable, and precisely integrated with business objectives. Over 80 percent of the Fortune 500 relies on our storage automation products to manage their complex storage systems. And by automating manual tasks required to discover, inventory, provision, and reprovision server resources, Symantec server automation products streamline administration and improve server utilization.

VERITAS CommandCentral™ Availability (now from Symantec)

Application availability management for the enterprise

- Improves application availability while increasing administrator efficiency
- Facilitates the management of clustered servers by ensuring that clusters are configured correctly
- Helps find and prevent human errors, and identifies failures based on historical data to avoid repeating mistakes
- Automates cluster operations so administrators can resolve problems faster and devote more time to areas that affect the bottom line

VERITAS CommandCentral™ Service (now from Symantec)

IT service delivery portal

- A centralized, Web-based portal that empowers IT organizations to manage and monitor their storage, backup/recovery, and CPU usage across the enterprise
- Permits visibility of the entire infrastructure, allowing IT organizations to understand which components of their environment are under- or overutilized
- Provides monitoring of the storage and backup environments plus a process automation engine that can be configured to provide standardized, repeatable services that are tracked and audited
- Presents business-level metrics for services throughout the organization

VERITAS CommandCentral™ Storage (now from Symantec)

Transforming SRM into storage as a service

- Application-centric storage management provides a highly centralized approach to managing storage, which increases the accountability of IT
 - Policy-based management ensures that service levels are met by alerting IT teams to any issues before they become critical
 - Provides in-depth view into storage and device details not easily obtained through manual processes
 - Addresses the critical issue of decreasing the time it takes for new storage to be provisioned or assigned to an application and brought online
 - Supports many industry standards, including the CIM/SMI-S storage management standard
-

VERITAS OpForce™ (now from Symantec)

Simplify server deployment

- Automatically discovers new (bare metal) servers as well as active servers
 - Saves an operating system snapshot that can be used to provision multiple servers with an identical configuration
 - Discovers software currently installed on each server and deploys additional applications to those servers
 - Centralizes all OpForce functions in a Web browser that can be securely accessed from anywhere
 - Supports most major operating systems and server devices including Solaris, AIX, Windows, Red Hat® Linux, and SUSE Linux
 - Can also configure appropriate network settings such as IP address, host name, and DNS
-

VERITAS Storage Foundation™ (now from Symantec)

A complete solution for online storage management

- Combines industry-leading Volume Manager™ and File System™ to provide a complete solution
- Automates manual storage management tasks, simplifies server migrations, and optimizes application performance
- Allows administrators to move data between different operating systems and storage arrays, spread I/O across multiple paths to improve performance, and identify and move unimportant or out-of-date files to inexpensive storage
- Limits the amount of time administrators need to take storage offline to perform regular maintenance functions
- Integrates with the leading hardware and software packages for a seamless datacenter

VERITAS Storage Foundation Cluster File System™ (now from Symantec)

Unleash the full potential of SAN technology

- File system accessibility from multiple servers helps reduce failover time in case of server failover
 - Cluster-wide freezing of the file system state enables operations requiring a consistent, on-disk image of a file system
 - Simultaneous access to storage from multiple servers allows load sharing between servers and enables full utilization of enterprise RAID subsystems
 - Cluster-wide logical device naming simplifies the management of SAN-based storage
 - Consistent logical views of volumes from all servers provides centralized management of cluster volumes
-

VERITAS Storage Foundation™ for Databases (now from Symantec)

Powerful manageability, high availability, and superior performance for DB2, Oracle, and Sybase databases

- Combines the industry's leading volume management and file system technologies
 - Improves manageability by automating many of the manual tasks associated with database storage management, thereby reducing administrative workload as well as human and operational errors
 - Enables administrators to set policies that classify company data based on various attributes, such as file size or age, and move the data to appropriate classes of storage
 - Allows administrators to use configuration templates to create or grow database storage environments quickly and accurately
 - Improves the overall performance of database environments
 - Protects essential data from system and subsystem failures, reducing costly downtime
-

VERITAS Storage Foundation™ for Oracle RAC (now from Symantec)

The most manageable RAC solution in the industry

- Provides an integrated solution optimized for Oracle Real Application Clusters
- Includes Cluster File System, Cluster Volume Manager, and Cluster Server to help implement robust, manageable, and scalable Oracle RAC
- Delivers the industry's first heterogeneous cluster file system supporting Oracle RAC on the Solaris, Linux, AIX- and HP-UX operating systems
- Dramatically simplifies the installation and ongoing management costs of an Oracle RAC environment
- Gives administrators the flexibility to create clustering solutions using best-of-breed storage hardware, allowing organizations to adapt to their changing technology requirements and contain costs

VERITAS Storage Foundation™ for Windows
(now from Symantec)

Advanced volume management technology for Windows

- A powerful, easy-to-use tool for maximizing the performance, availability, and manageability of diskstorage
- Provides scripting capabilities to automate repetitive tasks
- Reduces downtime for storage administration and growth without rebooting the server
- Allows software RAID capabilities to be combined with hardware RAID to provide the optimum storage resource for applications
- Simplifies operations for centralized, cross-platform management, reducing storage administration and training costs
- Increases throughput and bandwidth while providing scalable performance and balancing of application data loads
- Enables easy storage migration from server to server

Storage and Systems Management: Equally important as data backup and disaster recovery is fast system recovery and change management. Effectively managing network systems—be it patch management, OS deployment, or quickly restoring systems to a previous state helps ensure effective compliance with corporate policy standards and protection of critical assets. To keep business operations running and highly available, IT personnel know how important it is to handle these tasks quickly and with limited or zero impact. Regardless of the storage or systems management task, Symantec can provide a solution to ensure fast and reliable performance.

STORAGE MANAGEMENT

Symantec LiveState™ Recovery

Symantec LiveState Recovery is a family of suites, clients, options and add-ons providing innovative disk-based, bare-metal system recovery which combines revolutionary technologies for hardware-independent restoration and lights-out operation delivering unparalleled freedom to restore systems anytime, from anywhere, to any device.

Restore Windows® systems anytime, from anywhere to virtually any device

- Rapidly recover entire systems to dissimilar hardware platforms or even to virtual environments with the Restore Anywhere Option
- Easily restore servers in remote, unattended environments to meet recovery time objectives with the LightsOut Restore Option
- Create Backup Exec jobs directly in LiveState Recovery Manager, allowing established recovery point storage locations to be automatically backed up to tape
- Recover bare-metal systems in minutes and capture hot system recovery points to eliminate backup windows
- Centrally manage system protection and recovery status for thousands of remote systems with LiveState RecoveryManager (for servers and desktops)
- Automatically adjust recovery point routines to occur prior to a new application installation, user logon/ log off or specified change in megabytes of storage
- Set databases that are Microsoft Volume Shadow Copy Service (VSS)-aware to a quiet state during snapshots without actually taking them offline
- Adjust system usage performance in scheduled jobs or dynamically to more effectively utilize resources
- Save recovery points to virtually any disk-storage device
- Scheduled/automated recovery point creation
- Mount recovery point files as read-only drives that can be shared and accessed by others

- Symantec LiveState Recovery is part of the LiveState family of Windows server and desktop management solutions including provisioning, configuration management, patch management, asset management, and remote control.

Available suites:

- LiveState Recovery Advanced Server Suite—includes Advanced Server, Restore Anyware Option, LightsOut Restore Option, and Manager for Servers.
 - LiveState Recovery Desktop Suite—includes Desktop, Restore Anyware Option, and Manager for Desktop
-

Symantec LiveState Recovery—Restore Anyware Option

- Dissimilar hardware restoration—Combines hot imaging with the ability to restore to different hardware platforms (including different storage controllers and hardware abstraction layers) on the fly. This is also useful for upgrading hardware or for repurposing systems to serve a different role.
 - Convert the virtual—Users are provided tools and instructions on how they can convert their existing machine into a VMDK file and even restore recovery points to virtual environments in VMWare.
 - Users can restore the image in virtual environments to make changes, test patches and application installations or scan it for viruses and then save the updated recovery point out to a file format that LiveState Recovery can use to restore it to a physical system.
-

Symantec LiveState Recovery—LightsOut Option

- Easily restore servers in remote, unattended environments and distributed locations from a Windows desktop, laptop or Pocket PC using the LightsOut Restore Option.
- Eliminates the need for travel or onsite assistance to remote devices or headless servers in data centers by leveraging baseboard management controllers on standard servers (e.g., Dell Remote Access Card—DRAC or HP Integrated Lights-Out—iLO)
- With this option installed administrators can also add additional drivers directly to the Symantec Recovery Disk files located in the boot volume subdirectory offers more flexibility for easily recovering systems with the latest hardware devices (NIC cards, storage controllers, etc.), and eliminates the need for a new recovery CD to be built.

Symantec LiveState Recovery Manager

(for servers and for desktops)

- Centrally monitor backup status for an entire network, including how many devices are enabled for recovery, how many have jobs scheduled, how many have missed scheduled jobs and how many are offline
 - Displays all locations where recovery points are stored. Administrators can create Backup Exec jobs within LiveState Recovery Manager for these specific storage locations.
 - Use wizards to define backup policies for groups of servers or users with similar requirements and then deploy them through a drag-and-drop interface
 - Quickly resolve problems via centralized access to detailed storage information about each computer such as volume name, size, amount used, file system type as well as backup history and events including last backup time and last backup location
 - Jump-start backups on remote systems when backup jobs are not successful
 - Deploy and configure backup services on remote systems
 - Leverage Symantec pcAnywhere to remotely restore files, folders, non-system volumes or perform a full system recovery
 - Remotely verify backup integrity for all servers and workstation
-

Symantec PartitionMagic™ Pro

Create, resize, merge, and convert partitions without destroying data

- Protect valuable corporate information by segregating data from applications and operating systems; simplifies backup
 - Safely manage multiple operating systems
 - Convert from one file system or partition type to another without losing data
 - Test new or unstable software in a separate partition
 - Create, copy, resize, and delete partitions on hard drives up to 80 GB; this can also be done remotely across a TCP/IP connection
 - Create and run scripts to automate common partitioning tasks
-

Symantec VolumeManager™

Reliable disk storage management for Windows NT® and 2000 servers

- Copy, move, resize, format, or delete volume sets or partitions faster and safer than doing the same operations with a backup and restore operation
- Remotely monitor volume/partition and server information via Symantec StorageMonitor, which provides centralized server resource reporting
- Maximize existing storage space and lower the overall total cost of storage space by enabling easy volume set support and secure splitting and merging of FAT/FAT32 partitions
- Simplify the management-intensive backup process by simply moving or copying the entire Windows system, including hidden files and directory settings to new drive
- Securely shred partitions to ensure corporate confidentiality
- Create scripts to automate administrative tasks

SYSTEMS MANAGEMENT

Symantec Discovery™

Next-generation network inventory, asset management, software usage, and license management

- Agent-less discovery of all network devices
 - Agent-based inventory of hardware (CPU, memory, disk, etc.) and software (OS, applications, service packs, drivers, etc.)
 - Comprehensive audit trail for tracking installations, moves, additions, and changes
 - Patented LANProbe identifies physical location by interrogating switching and routing devices
 - Detailed Web-based reporting with configurable levels of access security
 - Supports Windows, Linux, UNIX, Mac OS® X
-

Symantec Ghost™ Solution Suite

Enterprise imaging and deployment solution with ease-of-use for managing the entire PC lifecycle, including OS deployment, software distribution, PC migration, and retirement

- Includes three applications in one suite: Symantec Ghost Corporate Edition, Symantec DeployCenter™ Library, and Symantec™ Client Migration
- Hardware and software inventory data is gathered from the Symantec Ghost Console, enabling administrators to design provisioning tasks based on specific client attributes
- Client Staging Area dynamically created on managed PCs provides the ability to launch and execute contents locally; store whole disk images, software hot fixes, and user profiles; and preserve contents during a cloning or restore
- Symantec Client Migration empowers IT administrators to migrate Windows OS and application settings, and user data—quickly and securely
- GDisk ensures that confidential data cannot be recovered from recycled, retired, or leased PCs via secure disk wiping to DoD requirements
- Upgrade to Symantec LiveState™ Delivery solution for enterprise-class scalability in highly distributed and heterogeneous environments (Windows, Linux, UNIX, Pocket PC)—including mobile and remote users—while leveraging your existing investment in Symantec Ghost images and AutoInstall packages

Symantec LiveState Client Management Suite

Comprehensive lifecycle management that enables organizations to discover, design, deliver, and secure client devices

- Includes the following products: Symantec Discovery, Symantec LiveState Designer, Symantec LiveState Delivery, Symantec LiveState Patch Manager, Symantec Ghost™ and DeployCenter imaging, Symantec pC Anywhere for Symantec LiveState, and Symantec Client Migration
 - Discover and inventory hardware and software assets
 - Design and create images and installation/configuration packages and scripts to automate client management tasks
 - Provision, configure, migrate, update, and patch thousands of devices simultaneously from centralized administration servers
 - Manage devices in a distributed and heterogeneous environment
-

Symantec LiveState™ Delivery

(Server and Desktop editions)

Scalable and reliable change and configuration management for client devices in heterogeneous environments

- Manages geographically distributed computers and devices from one central location using a single interface
 - Provides full life cycle management of computers and devices, including OS provisioning, application deployment, ongoing updates such as security patches, one-click system rebuild, and de-provisioning
 - Manages computing devices such as servers, desktops, laptops, handheld devices, Internet kiosks, and POS terminals
 - Designed for centralized management over wired and wireless LANs, WANs, and the Internet
 - Leverages existing images and installation packages such as MSI, WISE, and InstallShield
 - Supports Windows, Linux, UNIX, Apple® Mac OS X, and Pocket PC
-

Symantec LiveState™ Delivery Enterprise Manager*

Dynamic, policy-based client management

- Enhances Symantec LiveState Delivery by adding dynamic policy-based client management
- Designs, implements, and administers policies to manage a client's desired state
- Provides global view of entire enterprise and can drill down to a single computer
- Automates the removal of unauthorized software
- Integrates with Microsoft Active Directory®, asset management databases, in-house SQL databases, and other external sources
- Easily create target groups, queries, and policies

*Optional add-on component to Symantec LiveState Delivery. Requires professional services implementation.

Symantec LiveState™ Patch Manager

Automated solution for patch management and remediation

- Automate patch scanning and deployment without end-user intervention
 - Download required patches to a local patch repository to conveniently and efficiently provide ongoing access to patches and related information
 - Target specific user groups with flexible sorting and dynamic grouping capabilities
 - Dynamic Bandwidth Throttling detects network load and adjusts usage to limit bandwidth consumption
 - Checkpoint Restart ensures that patch deployments are successfully delivered even if transmission connections are interrupted
 - Patch status reports allow you to review scan results and client vulnerability states
-

Symantec pcAnywhere™ Corporate Edition

Fast and secure problem resolution for remote workstations and servers

- Industry-leading remote control combined with remote management, advanced file transfer capabilities, and robust security helps to quickly resolve help desk and server support issues
- Linux Host allows you to remotely manage Linux as well as Windows systems, freeing you from command-line Linux tools
- Symantec pcAnywhere Web Remote™ allows you to manage both platforms from a Java-enabled Web browser running on a system of your choice
- Symantec pcAnywhere Mobile™ allows you to access a pcAnywhere host from your Microsoft Pocket PC device over any TCP/IP connection, wired or wireless, with new, powerful, efficient file transfer capabilities that let you transfer files across different platforms
- Support for the Microsoft Windows Preinstallation Environment helps you get crashed systems back up and running quickly
- Built-in AES 256-bit encryption

Virus Protection, Antispam, and Content Filtering: Symantec has industry-leading virus protection, antispam, and content filtering solutions to safeguard the enterprise—all the way from the Internet gateway down to individual clients, and everywhere in between. A comprehensive product family protects essential servers, desktops, remote clients, and popular environments such as Microsoft® Exchange and Lotus® Domino® from viruses, worms, Trojan horses, blended threats, spyware, spam, and other malicious content.

Symantec AntiVirus™ Enterprise Edition

Comprehensive threat protection for every network tier, including client-based spyware protection, in a single, easy-to-deploy solution

- Provides advanced enterprise-wide virus protection, content filtering, and spam prevention for the groupware server and gateway, and virus and spyware protection for enterprise workstations and network servers
- NEW! Enhanced client protection from spyware and adware, including:
 - Real-time protection to reduce the risk of spyware reaching the system
 - Automatic removal for easy disposal of security risks
 - Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find spyware infection
 - Control over spyware settings via existing Symantec AntiVirus Corporate Edition management interface
- NEW! Enhanced client tamper protection guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures
- Mass-Mailer Cleanup automatically eliminates entire messages infected with mass-mailer worms, not just attachments
- NEW! Optional integrated Symantec Premium AntiSpam add-on subscription service provides best-of-breed spam prevention, including:
 - Regular updates to achieve 95% detection with less than one false positive for every million emails analyzed^{1,2}
 - Low administrative overhead and no additional software to install
 - Backed by Symantec Security Response, the world's leading Internet security research and support organization

¹eWeek 2003

²Yankee Group 2004

Symantec AntiVirus™ Corporate Edition

Automated defense and response against the latest viruses and spyware throughout the enterprise

- Advanced, enterprise-wide virus protection and monitoring from a single management console
 - NEW! Enhanced protection from spyware and adware, including:
 - Real-time protection to reduce the risk of spyware reaching the system
 - Automatic removal for easy disposal of security risks
 - Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find spyware infection
 - Control over spyware settings via existing Symantec AntiVirus Corporate Edition management interface
 - Backed by Symantec Security Response, the world's leading Internet security research and support organization
-

Symantec AntiVirus™ for Caching

For more information regarding additional Symantec Certified and Compatible Technology Partners that have developed integrations with Symantec AntiVirus Scan Engine, visit www.symantec.com/technologypartners or <http://enterprisesecurity.symantec.com>.



Fast, scalable, and reliable virus protection for application files on caching devices

- Provides scalable and reliable virus protection for traffic served through, or stored on, caching devices
- Enables administrators to remotely manage virus protection, as well as configuration, logging, reporting, and alerting
- Virus protection for both HTTP and FTP/HTTP traffic
- Employs award-winning Symantec technologies, including Symantec AntiVirus™ Scan Engine, to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats
- Support for version 1.0 of the Internet Content Adaptation Protocol (ICAP 1.0), an industry standard that allows the deployment of antivirus services at the gateway with minimal network latency
- Certified for leading caching devices, including Blue Coat ProxySG, Network Appliance NetCache®, and Cisco ACNS content engines

Symantec AntiVirus™ for Clearswift™

For more information regarding additional Symantec Certified and Compatible Technology Partners that have developed integrations with Symantec AntiVirus Scan Engine, visit www.symantec.com/technologypartners or <http://enterprisesecurity.symantec.com>.



Advanced, high-speed virus scanning and repair services for email (SMTP) and Web (HTTP) traffic for Clearswift CS MIMESweeper™ for Web, CS MAILsweeper™ for SMTP, or ES ClearEdge™

- Award-winning Symantec technologies optimized for speed, with minimal demands on the existing network infrastructure
- Seamlessly integrates core Symantec antivirus technologies such as NAVEX™ and LiveUpdate to automatically deliver and install virus definition and engine updates—without interruption to virus scanning
- Flexible installation, policy management, alerting, and reporting via both the Clearswift solutions and the Symantec AntiVirus Scan Engine administrative interface
- Easily accommodates increasing traffic volumes with automatic load-balancing
- Runs on Sun™ Solaris, Red Hat Linux, and Microsoft Windows 2000/Windows Server™ 2003 platforms
- Backed by Symantec Security Response, the world's leading Internet security research and support organization

Symantec AntiVirus™ Gateway Solution

Virus protection, spam prevention, and content filtering for Web and email traffic at the Internet gateway

- Combines two industry-leading Symantec solutions for comprehensive, multilayered protection against viruses, spam, and unwanted email and Web content at the Internet gateway
- Auto-learned whitelist automatically captures known and trusted mail domains to generate a comprehensive, effective whitelist and reduce false positives
- Enhanced heuristic antispam engine for greater effectiveness
- Flexible, customizable filtering rules scan message body text for keywords and phrases, eliminating spam and other undesirable content
- Mass-Mailer Cleanup automatically eliminates entire messages infected with mass-mailer worms—not just attachments
- Additional spam tagging and handling options offer greater flexibility

Symantec AntiVirus™ for Handhelds—Corporate Edition

Comprehensive, reliable protection for Palm OS and Pocket PC handheld devices

- Award-winning Symantec antivirus technologies protect handheld-resident data against malicious code downloaded from the Web, sent via email or Wi-Fi connection, or beamed via Bluetooth or infrared ports
- On-device alerting to respond to potential threats
- Automatic and up-to-date virus definitions via LiveUpdate
- Optimized to preserve handheld and network performance
- Backed by Symantec Security Response, the world's leading Internet security research and support organization

FOR DESKTOP SYNCHRONIZED DEVICES

(Version 3.0*)

- Single, transparent deployment of virus definitions to desktops with Symantec AntiVirus Corporate Edition installed
- Event and Configuration Manager (included) provides centralized control with configuration, implementation, and enforcement of policies from a single console
- Event and configuration console can be used to view multiple security products

* For U.S. customers only

FOR WIRELESS DEVICES

(Version 3.3)

- Leveraging existing mobile device management system infrastructures, administrators can deploy, manage, and update the device-resident antivirus client on mobile devices without desktop synchronization

Symantec AntiVirus™ for Microsoft® Internet Security & Acceleration (ISA) Server 2000

High-performance, scalable, and reliable virus protection for Web and SMTP traffic

- Employs award-winning Symantec technologies to provide scalable and reliable virus protection for Web and SMTP traffic
- Designed specifically to protect traffic served through the Microsoft Internet Security and Acceleration (ISA) Server 2000
- Easily configured to protect users from blended threats in all major file types, including compressed fileformats
- Leverages ISA Server's existing alerting capabilities
- Includes advanced features to block email-borne viruses before a cure is available
- Supports both stand-alone and array implementations of the ISA Server for flexible deployment

Symantec AntiVirus™ for Microsoft® SharePoint®

Protects portal environments from viruses, worms, and Trojan horses

- Protect Microsoft Office SharePoint Portal Server and Windows SharePoint Services from viruses, worms, and Trojan horses in all major file types
 - Integrated LiveUpdate functionality automatically updates virus definitions without interrupting virus scanning
 - Provides remote administration for virus protection, configuration, logging, reporting, and alerting
 - Easily accommodates growing traffic volumes with automatic load-balancing and licensing configurations for both internal and external users
 - Backed by Symantec Security Response, the world's leading antivirus and Internet security research and support organization
-

Symantec AntiVirus™ for Network Attached Storage

For more information regarding additional Symantec Certified and Compatible Technology Partners that have developed integrations with Symantec AntiVirus Scan Engine, visit www.symantec.com/technologypartners or <http://enterprisesecurity.symantec.com>.



Fast, scalable, and reliable virus protection for application files on network attached storage devices

- Enables administrators to remotely manage virus protection, as well as configuration, logging, reporting, and alerting
 - Allows administrators to redirect all irreparable, virus-infected files to a safe area on a centralized server
 - Provides scalable and reliable virus protection for valuable data stored on network attached storage devices
 - Employs award-winning Symantec technologies, including Symantec AntiVirus™ Scan Engine, to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats
 - Virus definitions and engines are updated automatically using Symantec LiveUpdate, with no interruption in virus scanning
 - Certified for leading network attached storage devices, including Network Appliance Filer, Hitachi Lightning NAS Blade, and Sun StorEdge™ 9900 NAS Blade
-

Symantec AntiVirus™ Scan Engine

Fast, scalable, and reliable content scanning services and API to protect against viruses and other unwanted content

- Easily integrates with third-party software and hardware via version 1.0 of the ICAP protocol or client ICAP API
- Enables third-party hardware/software vendors and ISPs to add value to their offerings by supporting Symantec's URL filtering and industry-leading antivirus technologies
- Virus definitions, engines, and URL content are updated automatically with no interruption in scanning
- Accommodates growing traffic volumes with automatic load balancing
- Runs on Sun Solaris, Red Hat Linux, SUSE Linux, and Microsoft Windows 2000/Server 2003 platforms

Symantec Brightmail AntiSpam™

Protects against spam, email-borne viruses, and other unwanted email

- Stops spam attacks in real time without compromising accuracy
 - Multilayered spam protection leverages over 17 different filtering technologies, including spam signatures, heuristics, reputation filters, language identification, and many proprietary methods
 - Flexible spam management and mail policies let IT administrators customize and enforce spam and unwanted mail handling for different groups or users in an organization
 - Intuitive Web-based control center enables powerful administration, centralizing and consolidating the management, customization, configuration, and monitoring of all parts of the system
 - Consolidated reporting gives administrators visibility into aggregated filtering performance for deployed servers
 - Administrators can quickly create custom organization-wide content filters to handle messages based on content, sender information, or other criteria
 - Comprehensive threat protection helps consolidate email threat management and monitoring via optional virus scanning and cleaning
-

Symantec™ Client Security

Proactively protects against blended threats through robust client protection, centralized management, and ease of administration

- Integrated security technologies proactively protect enterprise client systems from security risks and network intrusions
- NEW! Generic Exploit Blocking enhances intrusion prevention capabilities, resulting in reduced time-to-protection after vulnerability announcements
- NEW! Optimized out-of-the-box firewall configurations minimize configuration efforts while stopping the majority of threats
- Backed by Symantec Security Response, the world's leading Internet security research and support organization
- NEW! Enhanced protection from spyware and adware, including:
 - Real-time protection to reduce the risk of spyware reaching the system
 - Automatic removal for easy disposal of security risks
 - Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find spyware infection
 - Control over spyware settings via existing Symantec AntiVirus Corporate Edition management interface

Symantec™ Client Security for Nokia® Communicator

Threat protection through integrated antivirus and firewall technologies for Nokia Communicator business devices

- Protects Nokia 9500 Communicator business devices from unwanted network intrusions, as well as from viruses, Trojans, and worms
 - Allows IT to extend existing security policies to Nokia Communicator devices to mitigate threats and protect existing infrastructure
 - Centralized management enables administrators to configure, lock, and enforce security policies, either remotely or locally
 - Wireless security and application updates via LiveUpdate keep on-device protection current
-

Symantec Hosted Mail Security

Hosted email security solution powered by industry-leading antispam and antivirus technologies

- Powered by industry-leading Symantec Brightmail AntiSpam and Symantec AntiVirus technologies for effective spam and virus protection
- Hosted solution reduces the IT burden associated with managing on-premise solutions and allows companies to deploy their resources more effectively
- Decreases IT expenditures for additional hardware, bandwidth, and storage required for gateway email security
- Administrator and end-user quarantine that includes both Web-based and automated email digest options allows end users to manage their quarantined email and frees IT managers from having to address individual quarantine issues
- Content-filtering features include attachment blocking, subject and message body filtering, and encrypted file handling
- Content compliance features make it easy for organizations to control sensitive email content and enforce content rules to conform to IT, HR, or regulatory requirements

Symantec™ Mail Security 8100 Series



Email security appliance that controls spam traffic—stopping spam at the source

- Reduces total email volume up to 50% by stopping spam before it enters the network, while ensuring the continuous flow of legitimate mail
- Shapes traffic at the TCP protocol level by prohibiting spammers from forcing mail into a protected network. This causes mail to back up on the spammers' servers so that their infrastructure rather than yours incurs the burden of spam
- Contains escalating mail infrastructure costs by lowering administrative hardware, storage, and network overhead
- Scales to meet the needs of growing businesses. A single appliance handles up to 750,000 user accounts and email loads in excess of 30 million messages a day
- Couple with any antispam gateway solution, including Symantec Mail Security 8200 Series appliances, to provide a comprehensive multilayered approach to combat spam
- Powered by Symantec Brightmail AntiSpam technology and response, which protects over 300 million email user accounts. Monitors, detects, and responds to new spamming techniques and traffic patterns

Symantec™ Mail Security 8200 Series



Email security appliance with integrated, industry-leading antispam and antivirus technologies

- Powered by industry-leading Brightmail AntiSpam and Symantec AntiVirus technologies for effective spam and virus protection
- Appliance form factor and automatic updates enable easy, low-cost deployment and management
- Email firewall technologies reduce email infrastructure costs by restricting connections from spam-sending servers
- Content compliance features allow administrators to gain control over inbound and outbound email content
- All email security appliances can be managed from a single console
- Predefined reports provide insight into trends and attack statistics

Symantec™ Mail Security for SMTP

An integrated security solution that protects against viruses, spam, and other unwanted content

- Optional Symantec Premium AntiSpam add-on subscription service provides best-of-breed spam prevention—including a Web-based Spam Quarantine and Domino and Exchange Folder Agents—with low administrative overhead and no additional software to install
 - Mass-Mailer Cleanup automatically eliminates entire messages infected with mass-mailer worms, not just attachments
 - Basic spam tools include a heuristics antispam engine, custom filtering rules, and enhanced whitelisting, as well as additional spam tagging and handling options
 - Flexible, customizable filtering rules scan message body text for keywords and phrases, eliminating spam and other undesirable content
 - Custom Disclaimer allows administrators to insert custom text, such as a legal disclaimer, into outbound messages
 - Backed by Symantec Security Response, the world's leading antivirus and Internet security research and support organization
-

Symantec™ Mail Security for Domino®

(for Windows 2000 and Windows Server 2003)

An integrated security solution that protects against viruses, spam, and other unwanted content

- Optional Symantec Premium AntiSpam add-on subscription service provides best-of-breed spam prevention with low administrative overhead and no additional software to install
- Mass-Mailer Cleanup feature automatically eliminates entire messages infected with mass-mailer worms, not just attachments
- Basic spam tools include a heuristics antispam engine, custom filtering rules, and enhanced whitelisting, as well as additional spam tagging and handling options
- Provides proactive content filtering to automatically remove suspect emails with inappropriate attachment names, subject lines, extensions, or content
- Outbreak Notification alerts administrators to the first signs of a virus outbreak, allowing them to respond quickly
- Backed by Symantec Security Response, the world's leading antivirus and Internet security research and support organization

Symantec™ Mail Security for Domino® Multi-Platform Edition

(Windows, AIX, Solaris, iSeries™, and Linux platforms. Contains features noted above for Windows platforms, and antivirus/content filtering provided within Symantec AntiVirus™/Filtering for Domino for the other platforms.)

An integrated security solution that protects against viruses, spam, and other unwanted content

- Supports Domino 6 Server
 - Automatically detects and removes known and unknown viruses, including fast-spreading macro viruses
 - Protects against new viruses without requiring re-installation of software, reducing cost of ownership
 - Proactive content filtering automatically removes suspect emails with inappropriate attachment names, subject lines, extensions, or content
 - Includes Symantec Mail Security for Windows 2000/Windows Server 2003 and Symantec AntiVirus/Filtering for Domino
 - Supports AIX, Solaris, iSeries, and Linux
-

Symantec™ Mail Security for Microsoft® Exchange

An integrated security solution that protects against viruses, spam, and other unwanted content

- Optional Symantec Premium AntiSpam add-on subscription service provides best-of-breed spam prevention with low administrative overhead and no additional software to install
- Hourly virus updates using Symantec Rapid Release enable organizations to respond quickly to new threats
- Mass-Mailer Cleanup automatically eliminates entire messages infected with mass-mailer worms, not just attachments
- Basic spam tools include a heuristic engine, whitelists, and integration with Microsoft's Spam Confidence Levels and Intelligent Message Filter
- Incorporates rules-based content filtering to prevent unwanted content from entering—and confidential information from leaving—the network
- Backed by Symantec Security Response, the world's leading antivirus and Internet security research and support organization

Symantec™ Mobile Security for Symbian

Threat protection through integrated antivirus and firewall technologies for Symbian OS Series 60 and Series 80 supported smartphones

- Protects Symbian OS Series 60 and Series 80 smartphones from unwanted network intrusions, as well as from viruses, trojans, and worms
 - Allows IT to extend existing security policies to Symbian OS Series 60 and Series 80 smartphones to mitigate threats and protect existing infrastructure
 - Centralized management enables administrators to configure, lock, and enforce security policies either remotely or locally
 - Automatic wireless security and application updates via LiveUpdate keep on-device protection current
-

Symantec™ Web Security

High-performance content filtering and virus protection for the HTTP/FTP gateway

- Secures Web traffic with high-performance, integrated virus scanning and content filtering of HTTP and FTP traffic at the gateway
- Combines list-based techniques with heuristic, context-sensitive analysis tools for both virus protection and Web content filtering
- Simplifies administration and enhances management flexibility with new centralized multi-server policy management capabilities
- Manageable and scalable protection for individual users and groups via secure SSL support for external directory services, including LDAP, Active Directory, and Windows NT users/groups
- Reduces the amount of Web-based traffic, enhancing firewall and network reliability and performance
- Increases user productivity and ensures conformance with acceptable use policies by eliminating unwanted content

Norton AntiVirus™ for Macintosh®

The world's most trusted antivirus solution for Macintosh systems*

- Protects against PC as well as Mac viruses
- Quarantines suspicious files until they can be repaired
- AutoProtect finds viruses within file archives
- LiveUpdate downloads only needed virus definitions
- Automatically detects and removes viruses in Internet downloads, email attachments, file transfers, and other incoming files
- Easy installation starts protection right away
- LiveUpdate downloads new virus definitions and program updates automatically*
- New virus definitions take effect immediately
- Norton Scheduler allows scheduled virus scans

* One year of virus definition and scanning engine updates included with purchase of Norton AntiVirus for Macintosh; annual subscriptions available for subsequent updates.

Norton AntiVirus™ for Macintosh® with Symantec Administration Console for Macintosh

The world's most trusted antivirus solution for Macintosh systems

- Administration console centralizes enterprise-wide management of Mac clients protected with Norton AntiVirus for Macintosh 9.0 under OS X
- Administrators can view the security status of Mac clients, receive immediate notification of a virus event, and manage client installation and configuration from the console
- Protects against PC as well as Mac viruses, preventing Mac users from unknowingly spreading PC viruses to colleagues on the network
- Console utilizes stable open source technologies, including Apache Web Server, MySQL, and PHP
- Console uses standard Apple installation protocols for compatibility with Apple Remote Desktop and other software distribution tools

Vulnerability Management: Symantec vulnerability management solutions help IT organizations gain greater control over network infrastructure through the discovery, measurement, prioritization, and safeguarding of vulnerabilities. Symantec's advanced scanning and assessment technologies enable security administrators to proactively prevent the exploitation of potential breaches that threaten the security and availability of business systems and applications.

Symantec NetRecon™

Network vulnerability assessment with progressive scanning technology

- Scans multiple operating systems, including UNIX, Linux, Windows 2000, Windows NT, Windows 95/98, and NetWare
- Tests servers, firewalls, routers, hubs, switches, name services, network printers, Web servers, and other network devices
- Integrates with Symantec Enterprise Security Manager for host and network assessment and policy compliance
- Scans using many Windows NT/2000 network protocols such as TCP/IP, Novell® NetWare IPX/SPX, and Windows NetBEUI

Symantec™ Vulnerability Assessment

Gaining greater control over network infrastructure through the discovery, prioritization, and safeguarding of vulnerabilities

- Provides fast and thorough discovery of security vulnerabilities to quickly identify systems and applications at risk
- Delivers prioritized and up-to-the-minute vulnerability signatures and complete remediation information, allowing administrators to take proactive measures to effectively repair vulnerabilities most at risk
- Cost-effectively protects operating systems and applications—from a host perspective—eliminating false positives
- Utilizes the industry-leading vulnerability database from Symantec and employs the trusted, fast, and automated response capabilities of LiveUpdate and Symantec Security Response to identify threats recognized by CVE and Bugtraq™
- Tightly integrated with Symantec Security Management System, offering customers a common user interface, data repository, directory service, and agent

Symantec Consulting Services provides organizations with best practices security measures through comprehensive assessments, planning, and design consultations in order to deliver enhanced protection of critical business assets.

Symantec Advisory Services

Symantec Advisory Services offers consulting engagements focused on vendor-neutral solutions to security-related business problems. Our trusted advisors apply insight and expertise to help organizations develop proactive security risk management practices. The Symantec approach addresses the enterprise security lifecycle from strategy development to incident readiness, with a continuous focus on minimizing risks, stabilizing security costs, and reducing complexity.

Our consultants combine technical expertise with a business focus to create comprehensive solutions that are delivered with an emphasis on knowledge transfer, ensuring that every aspect of a project's findings can be successfully implemented and managed.

- Symantec Secure Application Services
- Symantec Secure Infrastructure Services
- Symantec Security Compliance Services
- Symantec Strategy Services
- Symantec Operation Services

Symantec Solutions Enablement Services

Symantec Solutions Enablement Services offers security product design and implementation services to optimize and accelerate the benefits of Symantec technology. Symantec security experts assess security technology needs, design optimal systems and architectures, and implement the appropriate products at the client, server, and gateway tiers.

Our consultants provide complete knowledge transfer services for Symantec enterprise security solutions, offering detailed security information and insights, as well as onsite training and custom services to help monitor and manage implementations.

- Symantec AntiVirus Services
- Symantec Client Security Services
- Symantec Enterprise Security Manager Services
- Symantec Gateway Security Services
- Symantec Incident Manager Services
- Symantec Security Technology Training

Symantec Managed Security Services: Symantec Managed Security Services provides remote security management and monitoring in order to maximize the efficiency of an organization's internal security staff. The outsourced services enable IT organizations to minimize security risks, increase operational efficiencies and staff productivity, and enhance regulatory compliance enterprise wide.

Symantec™ Managed Security Services leverages the Symantec Global Intelligence Network to offer fast and accurate analyses of security data to protect organizations from emerging threats and reduce overall security risk. A variety of popular service offerings is available to meet the specific operational requirements of most IT organizations:

- Monitored and Managed Firewall Services
- Monitored and Managed Network-based Intrusion Detection Services
- Monitored Host-based Intrusion Detection Services
- Monitored and Managed Integrated Security Appliance Services

Early Warning Services

Symantec Early Warning Services delivers timely security notifications and customized intelligence to meet an organization's specific security requirements. The services leverage the power of the Symantec Global Intelligence Network to provide organizations with a detailed view of vulnerability analyses, risk mitigation recommendations, and reliable insights that are tailored to their unique security environment. Symantec Early Warning Services consists of two service offerings that can be combined to meet the specific business needs of any IT organization:

- **Symantec DeepSight Threat Management System** delivers customized early warnings and mitigation steps on imminent threats headed your way. Focus resources on preventing attacks—not recovering from them. Protect critical systems before attacks hit.
- **Symantec DeepSight Alert Services** delivers personalized vulnerability and malicious code alerts to inform organizations of potential new threats. The alerts provide notification of vulnerabilities and exploits as they are identified, providing timely, actionable information and guidance to help mitigate risks before they are exploited.

Powered by the Symantec™ Global Intelligence Network

At the heart of Symantec's worldwide organization is the industry's most extensive security research infrastructure—the Symantec Global Intelligence Network. The Symantec Global Intelligence Network combines security intelligence, trusted expertise, and a global presence to enable enterprises and consumers to take timely action against today's security threats and stay ahead of tomorrow's vulnerabilities to improve their network security—all without jeopardizing their security budget.

Here's how: The Symantec Global Intelligence Network aggregates, analyzes, and delivers timely security notifications and recommended actions on security threats worldwide. Leveraging the insight and intelligence the Symantec Global Intelligence Network provides, organizations can proactively mitigate risks and balance their information security and availability to meet the changing needs of their environment.

The Symantec Global Intelligence Network gathers malicious code data from over 150 million desktop antivirus sensors and 20,000 intrusion detection (IDS) software and firewall sensors in 180 countries, and collects and analyzes data from 4,300 monitored and managed security devices around the world. The network leverages one of the world's largest vulnerability databases—covering 18,000 applications and operating systems from over 2,200 vendors and 2 million decoy email addresses scanned on a daily basis for antispam, phishing, and email security threats—to provide Symantec Security Response analysts with an authoritative and unparalleled source of security data. Symantec Security Response centers, located in North America, Asia, Australia, and Europe, are manned by researchers who represent the most highly regarded security experts in the industry, offering customers 24x7 coverage for important security events. The diversity of threats and risks handled by Symantec Security Response places it at the forefront of security research.

Symantec, the Symantec logo, IMUNE, Information Integrity, LiveUpdate, Norton, Norton AntiVirus, Norton AntiVirus for Macintosh, Norton AntiVirus for Macintosh with Symantec Administration Console for Macintosh, Norton Personal Firewall, pcAnywhere, Symantec Advanced Manager, Symantec AntiVirus, Symantec AntiVirus Corporation Edition, Symantec AntiVirus Engine, Symantec AntiVirus Enterprise Edition, Symantec AntiVirus/Filtering for Domino, Symantec AntiVirus for Clearswift, Symantec AntiVirus for Handhelds—Corporate Edition, Symantec AntiVirus for Microsoft Internet Security & Acceleration Server, Symantec AntiVirus for Microsoft SharePoint, Symantec AntiVirus Gateway Solution, Symantec AntiVirus Scan Engine, Symantec Brightmail AntiSpam, Symantec Client Migration, Symantec Client Security, Symantec Client Security for Nokia Communicator, Symantec Clientless VPN, Symantec Decoy Server, Symantec DeepSight, Symantec DeepSight Alert Services, Symantec DeepSight Threat Management System, Symantec DeployCenter Library, Symantec Discovery, Symantec Enterprise Firewall, Symantec Enterprise Security Manager, Symantec Enterprise Security Manager, Symantec Event Manager for Intrusion Protection, Symantec Event Manager for Security Gateways, Symantec Firewall/VPN, Symantec Gateway Security, Symantec Gateway Security 300 Series, Symantec Gateway Security 400 Series, Symantec Gateway Security 5400 Series, Symantec Ghost, Symantec Ghost Solution Suite, Symantec Host IDS, Symantec Incident Manager, Symantec Security Information Manager 9500 Series, Symantec Intruder Alert, Symantec LiveState Delivery, Symantec LiveState Recovery, Symantec Mail Security, Symantec Mail Security 8200 Series, Symantec Mail Security for Domino, Symantec Mail Security for Microsoft Exchange, Symantec Mail Security for SMTP, Symantec Managed Security Services, Symantec ManHunt, Symantec NetRecon, Symantec Network Security, Symantec Network Security 7100 Series, Symantec PartitionMagic, Symantec pcAnywhere, Symantec Security Management System, Symantec Security Response, Symantec VolumeManager, Symantec VulnerabilityAssessment, and Symantec Web Security, VERITAS Application Saver, VERITAS Backup Exec, VERITAS Backup Exec for NetWare Servers, VERITAS Backup Exec for Windows Servers, VERITAS Backup Exec for Windows Small Business Server, VERITAS Bare Metal Restore, VERITAS Cluster Server, VERITAS Cluster Server QuickStart, VERITAS Cluster Server Traffic Director, VERITAS CommandCentralAvailability, VERITAS CommandCentral Service, VERITAS CommandCentral Storage, VERITAS Enterprise Vault, VERITAS Global Cluster Manager, VERITAS i3 for ClarifyCRM, VERITAS i3 for Oracle Applications, VERITAS i3 for PeopleSoft, VERITAS i3 for SAP, VERITAS i3 for Siebel, VERITAS InDepth for IBM DB2 Universal Database, VERITAS i3 for Oracle, VERITAS i3 for SQL Server, VERITAS i3 for .Net, VERITAS i3 for J2EE, VERITAS i3 for Web-J2EE, VERITAS i3 for Web Servers, VERITAS Insight Inquire, VERITAS NetBackup Enterprise Server, VERITAS NetBackup Server, VERITAS NetBackup Storage Migrator, VERITAS OpForce, VERITAS Replication Exec, VERITAS Storage Exec, VERITAS Storage Foundation, VERITAS Storage Foundation Cluster File System, VERITAS Storage Foundation for Databases (DB2, Oracle, and Sybase), VERITAS Storage Foundation for Networks, VERITAS Storage Foundation for Oracle RAC, VERITAS Storage Foundation for Windows, and VERITAS Volume Replicator are registered trademarks and/or trademarks of Symantec Corporation and/or its subsidiaries. Apple, Mac, Mac OS, Macintosh, and Rendezvous are trademarks or registered trademarks of Apple Computer, Inc. IBM, AIX, DB2, Domino, iSeries, and Lotus are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Microsoft, Active Directory, SharePoint, Windows, Windows Mobile, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Novell and NetWare are registered trademarks of Novell, Inc., in the United States and other countries. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Palm and Palm OS are registered trademarks or trademarks of PalmSource, Inc. or its affiliates. Sun, Java, JavaBeans, JVM, Solaris, and StorEdge are trademarks or registered trademarks of Sun Microsystems, Inc., in the U.S. or other countries. All other brand and product names are trademarks of their respective holder(s). Copyright © 2005 Symantec Corporation. All rights reserved. Printed in the U.S.A. Not all products are available in all countries. All product information and availability are subject to change without notice. 10/05

For more information on Symantec
products contact us at: 1 (800) 745 6054
www.symantec.com

For your convenience you can also shop
online at www.symantecstore.com/enterprise,
where you can easily download Volume
License Solutions for immediate use of
Symantec's most popular enterprise products.*

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com