

Small and Midsize Business Protection Guide

Close the protection gap and safeguard
your business future

The protection gap

Computers have long been indispensable for running a small or midsize business (SMB). Although information technology (IT) introduces new risks and management challenges, most businesspeople have a general understanding of its risks—and they do their best to address them. More often than not, this means using a network firewall, adding an antivirus and possibly an antispam solution, and implementing some sort of backup schedule.

Admittedly, it is difficult to run a business and keep protection up to date at the same time. New research documents the gap: a recent survey¹ showed that 33 percent of small and midsize businesses lack even basic antivirus protection, 47 percent fail to back up desktop PCs, and 20 percent maintain no server backups of any kind.

Yet the risks increase, and the business protection gap grows. More complex threats and attacks, some focused on individual businesses, have become routine. The value of data and the cost of losing it are both on the rise. Meanwhile, the technology environment keeps changing as wireless networks, mobile computing devices, Mac OS® and Linux® machines in the workplace, and Web gateway and server hardware are added to the infrastructure—and none of these additions are covered by basic protection.

Individual “point products” may meet specific requirements, but don’t work well together because:

- Duplication among separate products wastes money, time, and effort
- Gaps and uneven coverage leave critical assets and information at risk
- Solution management takes skills and time away from tasks that add more business value

To close their protection gaps, small and midsize businesses need reliable, comprehensive protection that have compatibility designed in; are sized right; are easy to install, configure, and use; and come from a source they can trust.

Evaluating your coverage

The sidebar “Phases of protection” outlines the progress of many small and midsize businesses from a patchwork of low-cost solutions toward a mature, scalable security and data protection infrastructure. While many small and midsize businesses have graduated to Phase 1 compatible solutions from a single leading vendor, many more try to make do with Phase 0 protection—cobbed together from solutions bundled into their hardware, operating systems, or ISP services—and rely on home-built backup and recovery methods. The following sections will outline the protection gaps such approaches can leave, and point out a few of the management challenges they introduce.

Phases of protection

This guide describes four phases of protection for small and midsize businesses:

Phase 0—“Do-it-yourself” multivendor protection, often assembled from point solutions included with PCs, Internet access services, and external hard drives. May leave coverage gaps; difficult to manage.

Phase 1—Single-vendor protection assembled from individual point solutions purchased as needed. Duplicate agents, processes, and consoles may slow performance and complicate management.

Phase 2—Single-vendor suites designed specifically to meet the requirements of small and midsize business. Consolidated and streamlined agents, processes, and consoles improve performance and manageability.

Phase 3—Advanced single-vendor solutions that extend the capabilities of suites to meet specific business requirements, and are customized by vendors’ technology partners for key-in-lock business alignment.

¹ Applied Research - West, Inc. *Storage and Security in SMBs: 2009 survey results*. (Cupertino, CA: Symantec Corp. March, 2009). http://eval.symantec.com/mktginfo/enterprise/articles/b-storage_and_security_in_smb_03-2009.en-us.pdf.

Endpoint Security

Technically, “endpoint” means the origin or destination of a TCP/IP or other transport layer connection. Practically, it means servers, desktops, laptops, and mobile devices that send or receive information. It is important to secure endpoints because devices and information now cross network perimeters routinely—for example, as employees connect at airports or coffee shops, contractors bring in their own laptops, or thieves try to establish a WiFi connection from your parking lot. Perimeter security is still important to defend against wholesale attack—but it is no longer enough.

Phase 1 endpoint security coordinates antivirus, firewall, intrusion prevention, and other protection to ease system, user, and management burdens.

Phase 2 protection goes one step further, integrating multiple solutions into an easy-to-administer whole:

- **Antivirus and anti-spyware** are the most familiar forms of endpoint protection. Today’s best solutions offer deep protection against insidious “rootkit” malware, operate using fewer system resources, and adapt to user performance requirements more effectively than ever before.
- **Network threat protection** is a host-based firewall that protects the network by enforcing network traffic rules instead of looking for signatures of past attacks. This type of endpoint protection blocks threats based on what they are designed to do, even if they have never been encountered before.
- **Proactive threat protection** is a rules-based client-side engine that serves as a final line of defense, even against brand-new threats.
- **Single-agent and single-console management** keep endpoint computing loads and administrative burdens manageable to coordinate security technologies with minimum investment of time and resources.

Phase 3 endpoint security enhances Phase 2 protection with additional solutions to meet specialized requirements—for example:

- **Network access control** in software or appliance format maintains and enforces policies granting or restricting network permissions, regardless of how the endpoints access resources.
- **Endpoint data-loss prevention** scans incoming and outgoing communications for critical patterns such as those of Social Security or credit-card numbers, enforcing policies that restrict how many critical patterns an individual message may contain or an employee may send.
- **Protection for specialized devices** covers the increasing number of Mac OS, Linux, and mobile devices found on today’s heterogeneous networks.

Messaging Security

Spam remains a waste and a menace, but Internet service providers’ Phase 0 antispam protection solutions have diminished the sense of urgency with which many small and midsize businesses approach it. Phase 1 solutions go further than ISP offerings, adding more effective filtering at the cost of a little more work for administrators.

But ISP protections fail against attacks focused on individual companies or people. And even the best Phase 1 antispam solutions are not designed to protect against inappropriate and legally risky content, confidential information, or malware transmitted through *outbound* email.

Phase 2 protection integrates multiple content controls such as these:

- **Scanning of outbound** as well as inbound traffic for viruses, spam, and phishing attacks
- **Content filtering** to keep sensitive, confidential, or inappropriate content from being sent, to cut risks of fraud, intellectual property theft, and unintentional disclosure of confidential information
- **Signature-based spam protection** with regular signature updates for real-time protection, even against new threats

Specialized Phase 3 solutions include:

- **Gateway antispam** in software, appliance, or new virtual appliance formats, to provide added protection and offload processing burdens from networks and clients
- **Protection for specialized servers** such as SharePoint and other content-management systems
- **Archiving and recovery** management tools for large email-intensive environments, or where regulatory or court-ordered e-discovery is a significant risk

Backup and Recovery

Many small and midsize businesses ignore backup and recovery processes, or treat them at most as a nagging concern. However, half of surveyed businesses have lost important business data such as financial, legal, and personnel records; service-level agreements; and information held on behalf of third parties. A third of them have lost business as a result. In the 25 percent of SMBs that perform no backups at all and in the more than 50 percent that store backup files in the same location as the computers they are intended to protect, these vulnerabilities persist.

Backups that use Phase 0 solutions such as copying to USB drives or portable media are inconvenient—especially in the middle of an urgent project, when the risk and cost of data loss are greatest. Moreover, file-based backups will not protect against system crashes—or make sure that all servers and workstations are backed up.

Phase 1 point solutions are a big step up. The best of them move backup copies to centralized network storage or secure storage online, while complementary point solutions offer system backup and recovery and even centralized management. But the greatest vulnerability—insufficient capability for timely and effective system recovery—remains.

Data and system protection in Phase 2 suites addresses management head-on, with capabilities such as these:

- **Background operation** to create full system backups while you work, with no interruption of productivity
- **Centralized monitoring** to show the backup status of every computer system on your network
- **Application protection** for critical Microsoft® mail, content management, and other solutions
- **Full system recovery**, including protection for virtual environments

Phase 3 solutions address special backup requirements of servers, remote offices, and databases, including the following:

- **Special requirements** to address industry-specific regulations and standards frameworks
- **Server solutions** that protect information stored in Web, database, and other critical servers
- **Unique capabilities** to meet the unique requirements of individual company business models

Symantec Protection Suite

Symantec has a more than 25-year history of helping customers to secure, back up, and recover critical business information; In addition to carefully monitoring the protection requirements of small and midsize businesses, the company—through the Symantec™ Global Intelligence Network—also watches the threats its customers face, and integrates its experience and research into a solution suite for small and midsize business customers based on these principles:

- **Complete protection**—multilayer coverage that moves beyond antivirus and basic backup to address today’s full spectrum of business requirements
- **Easy management**—streamlined technologies that deploy quickly, fit together seamlessly, and protect effortlessly
- **Confidence, always**—clear, automated processes and strong support for complete desktop and laptop recovery with minimal downtime so that businesses can avoid emergencies entirely, or face them with the assurance that comes from a solid plan and good tools

Symantec™ Protection Suite is an advanced Phase 2 solution that addresses the most pressing endpoint, messaging, and backup protection requirements of small and midsize businesses. Available in separate editions for small businesses with 5 to 99 employees and midsize businesses with 100 to 499 employees, it combines advanced capabilities available from no other source. These include:

- The industry’s longest unbroken record of flawless performance in independent tests of antivirus effectiveness
- Policy-based filtering of email and instant-message content
- Recovery of critical files or folders in seconds and of complete systems in minutes, even to different hardware or virtual systems
- Advanced manageability from coordination across technologies and a consistent management interface

Symantec Protection Suite is sold through and supported by Symantec Solution Partners—a worldwide team of security and data-protection specialists with the knowledge, experience, and resources to put the right solution in place. It provides an unmatched foundation for advanced Phase 3 solutions configured, implemented, and managed by local partners with a deep understanding of small and midsize business technology and business requirements.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website. 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

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Mac and Mac OS are trademarks of Apple, Inc., registered in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds. Microsoft is a U.S. registered trademark of Microsoft Corporation. Other names may be trademarks of their respective owners.
07/09 20050014