CHANGING RISKS, RISING COSTS

Information is fundamental to your business: You and your employees constantly exchange, update, and move customer records, messages, plans, contracts, invoices, financial data, and other information, some of it sensitive or highly confidential. But new mobile devices and tools—instant messaging, social networking sites, and collaboration platforms—blur the lines between business and personal computing, and can send or publish your information anywhere in less than an instant.

Protecting electronic information and communications against internal and external threats, data loss, downtime, or disaster is more than just important—it’s the foundation of your customer relationships, and the core of your business. But the technology keeps changing, and it’s easy to fall behind on protection. Consider these real-world scenarios:

- Email antivirus programs won’t protect popular Web mail, which uses different technologies—and is the fastest-growing source of online attack.¹
- Confidential information can leak out of a business invisibly on “thumb” drives, iPods, CD- and DVD-ROMs—and in email with the slip of a finger.
- Targeted attacks and phishing spam trick employees into voluntarily lowering defenses and disclosing private information—even when policies forbid it.
- Fire, equipment failure, flood, or sabotage can make information on a critical server unavailable for hours or days—or delete it forever.

Those risks are real—and for small and midsize businesses, the costs are high.

- 28 percent of customers have seen vendors shut down because of a disaster²—even four hours of downtime leads to significant revenue loss.³
- 26 percent of customers have lost important business data because of a vendor’s disruption.⁴
- Customers estimate that vendor downtime costs them $15,000 per day—and 42 percent have dropped vendors because of unreliable computer systems.⁵
- 33 percent of businesses report lost sales as a result of their own business disruptions, and 20 percent lost customers.⁶

If your business is operating without up-to-date protection that includes security and backup/recovery technologies, you risk losing critical information, customer relationships, and your hard-won reputation. At a minimum, your business needs better defenses against internal and external threats, with faster, more reliable recovery from disruption and disaster, to safeguard your customers, employees, and your business future.

TABLE OF CONTENTS

» Complete Business Protection ........................................................................................................ 3
» Best Practices .................................................................................................................................. 4
» Solutions to Protect Your Business Information ............................................................................. 5
» Compatible Symantec Solutions ..................................................................................................... 6
» Why Symantec? ............................................................................................................................... 7
» A Partnership You Can Count On .................................................................................................... 8

⁴ Symantec Corporation. SMB Disaster Preparedness Survey. Ibid.
⁵ Ibid.
A well-protected business combines multiple defenses against threats to computers and information, blocks unintended disclosure of confidential information, backs up critical information and systems—and does it all without breaking the budget or burdening business managers, employees, or technical staff.

Only Symantec offers complete protection, right-sized for your business, and ready to grow when you do. Get up-to-date solutions at a price you can afford to protect your business against:

**Online attacks** that disable computers, steal information, and defraud employees and customers. Antivirus protection is essential, but not enough to protect against the new generation of spam, viruses, and fraud and theft targeting information assets.

**Information loss** has grown so common that a few lost files, folders, and emails seem almost routine—until hardware failure, natural disaster, or catastrophic error exposes the real risk. Unmanaged or hit-or-miss employee-managed backup processes are unreliable and put your information at risk.

**Unintended disclosure** of confidential, sensitive, or proprietary information is embarrassing and expensive, damages your company’s reputation, and undermines customers’ trust.

**Inefficiency**, complexity, and cost to manage multiple single-purpose products drain valuable time, resources, and profit from your business, and leave you with unprotected gaps. Technology that requires constant attention takes your mind off your business—and that’s no bargain at any price.
BEST PRACTICES

No one set of rules can protect every business, but thoughtful owners and managers take steps like these:

1. **Close security gaps:** Laptops travel, and contractors and visitors connect to your network. Protect network endpoints, not just perimeters.

2. **Integrate defenses:** Combine antivirus, firewall, intrusion detection, and vulnerability management at endpoints, and add encryption if they travel.

3. **Patch software:** Threats evolve, so close vulnerabilities quickly by applying updates from Microsoft® and other software providers.

4. **Update virus definitions:** Keep your virus definitions up to date so your antivirus software recognizes new threats.

5. **Alert employees:** Warn them about attachments and links in unexpected email, and in software downloads before they are scanned for viruses.

6. **Don’t invite trouble:** File-sharing services and websites may install malicious code automatically. Stop them with training, policies, and software.

7. **Strengthen passwords:** Require passwords that mix letters and numbers—never names or dictionary words—and change them often.

8. **Schedule backups:** Implement and enforce backup schedules for your servers, desktops, and laptops—and automate as much as you can.

9. **Back up complete systems, too:** A “down” server means lost business, so back up the operating system, applications, configurations, and settings, not just files.

10. **Keep off-site backups:** Make sure files and systems can survive fire, flood, vandalism, sabotage, loss of your facility, or even a regional disaster.

11. **Test backups:** Don’t wait until recovery to discover a resource, process, or technical shortcoming—test the entire cycle.

12. **Get help:** Find a local IT partner whom you trust, who understands and can help with both your business and technical requirements.
Symantec builds industry-leading technologies and security intelligence into complete, scalable solutions right-sized for your business and budget. And Symantec is the only company that offers fully compatible solutions for critical endpoints, servers, gateways, and information from a single vendor.

**Symantec™ Endpoint Protection Small Business Edition**
Protects laptops, desktops, and servers from threats, spam, and phishing

- *Antivirus/antispyware* delivers up-to-date protection backed by intelligence from the world’s largest security network.
- *Personal firewall* defends every laptop, desktop, and server on your network, and blocks threats carried in on portable devices.
- *Privacy protection* safeguards employees from identify theft and online attacks.
- *Intrusion prevention* identifies and stops software that tries to tamper with your network.
- *Proactive threat scanning* blocks even new or customized threats based on their behavior and targets.

**Symantec™ Protection Suite Small Business Edition**
All the protection of Symantec Endpoint Protection, plus:

- Symantec™ Mail Security for Microsoft Exchange®
  Protects email at the server with industry-leading antivirus, antispam, and content filtering
  - Antivirus/antispyware blocks both known and previously undetected viruses and security threats in email.
  - Antispam/antiphishing provides high-accuracy defenses that keep useless, dangerous email off Exchange servers.
  - Email content filtering prevents costly leaks of confidential or sensitive information.

- Symantec Backup Exec™ System Recovery Desktop Edition
  Automated backup and quick recovery of Windows® laptops and desktops
  - Automated backups protect desktop and laptop computers without interrupting work.
  - Fast, simple recovery of a single file or folder or a complete Windows system—even to new hardware or a replacement system—in just minutes.
  - Home page view immediately identifies the backup status of computer systems.
  - Run backups automatically when the Symantec ThreatCon level reaches the threshold you specify.

- Symantec™ Protection Suite Advanced Business Edition
  All the protection of the Small Business Edition, plus:

- Symantec Backup Exec™ System Recovery Server Edition
  Protects critical servers automatically through scheduled or event-driven backups
  - Back up server images to off-site FTP locations or secondary disk drives for enhanced disaster recovery.
  - Protect and recover servers to physical or VMware®, Microsoft, or Citrix® virtual environments with seamless physical-to-virtual and virtual-to-physical conversions.
  - Recover systems to dissimilar or replacement hardware with Restore Anyware™ technology.

- Symantec Brightmail™ Gateway
  Inbound and outbound messaging security and data loss prevention for email and IM
  - Includes advanced antispam, antivirus, content filtering, and data loss prevention.
  - Scans inbound and outbound messaging traffic for compliance with regulatory and governance requirements.
  - Uses incident management and reporting to help analyze, manage, and control policy violations.
COMPATIBLE SYMANTEC SOLUTIONS

Keep pace with your changing business.

**Symantec pcAnywhere™**
Secure remote access and troubleshooting
- Remote access and control let you work away from the office or manage distant computers.
- Remote troubleshooting by your IT staff or Symantec partner gets PCs productive again, fast.

**MessageLabs/Symantec Hosted Services**
Secure managed email, Web, and IM communications
- Spam and virus blocking, email and Web misuse prevention, and email encryption with no need for on-site hardware or software.
- Easy to deploy and manage, with automatic updates and a comprehensive Service Level Agreement.

**Advanced solutions that grow with your business**
- Continuous data protection for mission-critical servers with zero-loss recovery
- Deduplication and archiving to reduce storage costs and management burdens
- Compliance solutions to enforce IT policies and reduce regulatory exposure
- Tamper protection to safeguard information on critical servers
- Advanced virtualization support for secure, efficient operation from the desktop to the cloud
- Green IT solutions to reduce power and cooling requirements and environmental impacts
- Consulting services to meet specialized industry or company needs
- Skilled local services, custom solutions, and support from more than 60,000 Symantec partners

*Every Symantec small business solution offers:*

**Automated Updates**
Keep systems protected without interrupting you or your employees.

**Consistent Processes and User Interface**
Install faster, operate more efficiently, and leave more time for business.

**Zero-Impact Design**
Run faster with lower CPU and memory impact, so you can do more with less.

**Support**
Links you to engineers with in-depth experience in availability and security.

**Global Intelligence**
Alerts you to threats from the Symantec™ Global Intelligence Network.

**Real-Time Response**
Draws on Symantec Security Response to identify and stop threats quickly.

**Confidence Always**
Backed by the world’s security, data protection, and management software leader.
You can rely on the world leader in security, data protection, and management software to protect your computers and information so you can focus on your customers, employees, and business operations. In an environment that puts your critical computing and information assets at risk, only Symantec offers single-vendor solutions to help you protect and manage critical endpoints, servers, gateways, and information.

**Protect completely**
Award-winning protection for business computers and information
- Protects desktops and laptops against online attacks.
- Safeguards information in both inbound and outbound email.
- Backs up critical information and systems for quick, granular recovery.
- Gives IT specialists a consistent interface to keep them effective.

Backed by the world’s largest network of security monitors to keep you protected from the latest threats.

**Manage easily**
Easy to purchase, set up, and use, solutions deliver protection in less than 20 minutes.
Consistent operation and interfaces mean solutions install quickly with no need for extra training.
Automated features like updates, backups, and data loss prevention operate in the background so they don’t interrupt workflow.

**Confidence always**
Leading technologies backed by local support.
The business world’s number-one choice for security, data protection, and management software.
Expert local assistance when you need it from more than 10,000 members of the Symantec Small and Medium Business Specialization program.
A PARTNERSHIP YOU CAN COUNT ON

Whether you purchase Symantec products individually or in convenient suites from a local Symantec partner or online, you can always count on complete protection to match your IT requirements and help keep your business going.

Symantec protects more systems, networks, and business information than any other company. Contact us today for a comprehensive solution for your business.

Select a solution from the Symantec Small Business Website.

Find a solution partner at the Symantec Partner Website.

Contact Symantec outside the United States through a Symantec Sales Office.

Call us for product information in the U.S. at +1 (800) 721 3934.

Visit the Symantec Business Online Store to learn more and buy your solution online.