THREE KEYS TO COST-EFFECTIVE SECURITY FOR YOUR SMALL BUSINESS
OVERVIEW

Data and communication protection isn’t a problem limited to large enterprises. Small and medium businesses are often at greater risk for attacks or data breaches as they’re less likely to have strong levels of protection in place. To compound matters, the cost of losing just one customer or failing a compliance investigation as a result of a security incident can mean the difference between business success and failure.

Data and device security don’t need to be complicated or expensive. In this e-book, you’ll learn how to protect your valuable assets without the expense or time commitment of building a full IT infrastructure.
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>KEY #1</td>
</tr>
<tr>
<td></td>
<td>You don’t need an IT infrastructure to protect your business</td>
</tr>
<tr>
<td>06</td>
<td>KEY #2</td>
</tr>
<tr>
<td></td>
<td>Start planning now to scale security as your business grows</td>
</tr>
<tr>
<td>09</td>
<td>KEY #3</td>
</tr>
<tr>
<td></td>
<td>Strong security can help you achieve regulatory compliance</td>
</tr>
<tr>
<td>12</td>
<td>Summary</td>
</tr>
</tbody>
</table>
You don’t need an IT infrastructure to protect your business
Cloud-based security helps small businesses utilize enterprise-grade security tools on a smaller budget while leaving management and maintenance to the vendor.

No matter your size, security is still an important issue
Although small and medium businesses generally don’t have an IT administrator, and even more rarely a staffed IT department, they must still address security threats, manage risk, and maintain compliance with regulatory and industry security mandates, just like their larger counterparts.

The challenges of managing security yourself
Even if it sounds simple to install an endpoint protection solution on your own network, realize you’ll also need servers, switches, and other hardware and software resources—and someone with the time, knowledge, and skills to manage and maintain the entire infrastructure.

Before you decide to take all that on in-house, assess if you have a resource who can be sure your server operating system is patched and up-to-date and your hardware has the latest firmware installed. You’ll also need someone to monitor server performance and troubleshoot network issues.

Cloud-based security: no dedicated IT resources required
If it sounds daunting and expensive to manage security yourself, consider a cloud-based security solution. A number of benefits make cloud-based security a great solution for businesses of all sizes, including flexible pricing and no requirement for dedicated IT staff, hardware, or management software.

Cloud-based security is cost-effective, affordable, and predictable, because a regular subscription fee replaces up-front expenses in hardware and software. By paying for only the services you need, you have flexibility to quickly scale up with company growth or meet spikes in demand.

Because most small and medium businesses don’t have resources with the knowledge, skills, and time to properly manage hardware, software, and the network back end, a cloud-based security solution makes perfect economic sense.

Security for remote employees
Cloud-based solutions also help address the security requirements of the increasingly distributed workforce. More employees are connecting to their networks from a remote location, which means security protection is required no matter where they’re based. A cloud-based security solution that provides automated system security updates for your employees’ systems whenever they connect to the Internet is the perfect answer.
Start planning now to scale security as your business grows
As your business grows, your IT security needs will grow right along with it. Here’s how to cut costs, boost productivity, and protect your customers with secure cloud services that scale with your business.

**Plan for growth AND security**

If you’re doing your job right, your business will grow. But not planning for the growth of your network and your data is a mistake that can cause significant security problems.

It’s important to take time to develop a solid strategy for growth, and consider how your decisions today will affect your business next month or next year. Cloud-based security solutions can give you the flexibility, security, and scalability your computing infrastructure needs.

As your business grows, chances are more users will need to access your network and systems. Whether working on site from your office, remotely from a home office, or across the country from a satellite location, your users’ PCs need solid security.
Critical security issues to consider

Here are some critical security issues to consider when planning for business growth:

**Protection**: No matter where your workers are located, their endpoints and precious data require protection. Computers are under virtually constant siege from malware, spyware, spam, phishing scams, and hackers.

Look for a cloud-based security solution managed from a Web-based console that will stop threats in their tracks. Be sure it will transparently protect your PCs and servers with the latest security updates whenever your staff is connected to the Internet.

**Cost**: Every time you add another worker, you pay the cost of protecting and supporting that user. If you buy your own servers, you may end up spending money on resources you don’t need today just to leave some room for future growth. Eventually, you’ll need to invest in additional hardware that most likely won’t be fully utilized.

Consider a cloud-based security solution that lets you purchase only the security protection you really need. As part of the regular subscription fee, you should receive support delivered by specialists twenty-four hours a day, seven days a week. And best of all, when you need to scale up or down, it’s easy to add or subtract services.

**Productivity**: Competition is fierce, and you need to be sure your workers have the flexibility to meet your customers’ needs. By embracing mobile computing and telecommuting, your users can connect from home offices or public Wi-Fi hotspots and work securely no matter where they’re located.

However, these productivity benefits come with increased risks, so be certain that your remote endpoint PCs are secure. Cloud-based security solutions ensure endpoint PCs are protected whenever they’re connected to the Internet.

Manage the growth of your business; don’t let the growth manage you. Develop a plan and take a look at cloud-based security to see it fits into your strategy and can help you grow the smart way.
Strong security can help you achieve regulatory compliance
Resolve to implement worthwhile security measures that achieve compliance instead of completing a simple checklist and crossing your fingers.

**Being compliant doesn’t mean you’re secure**
If your business is covered by one of the many federal regulations mandating data security, you probably spend a significant amount of time ensuring your company is in compliance. But many organizations are so focused on achieving compliance, they lose sight of the real goal: protecting their data.

It is possible to satisfy the minimum compliance requirements without being truly secure, especially when dealing with multiple, overlapping compliance directives. However, a better approach is to focus first on implementing the best security possible for your organization and achieving compliance as a byproduct of implementing a security solution.

**Compliance guidelines are often minimum baselines for security**
It can be a complex struggle to achieve compliance, especially for businesses that must meet multiple regulatory and industry mandates at the same time.

Some businesses may deal in financial matters and health insurance as well as accept credit card payments, thereby putting them under the gun for compliance with GLBA, HIPAA, and PCI DSS.

Each of these individual regulatory or industry compliance mandates was developed to address specific concerns. It would be logical to assume that if a business achieves compliance with a given set of directives, it is secure and properly protects its data. However, that is not necessarily true.

Achieving and maintaining compliance with data protection requirements is certainly better than nothing. But the regulations and guidelines are often broadly written, open to interpretation, and intended to create a minimum acceptable baseline—not an impenetrable web of security.

**The two basic steps to achieving security and compliance are:**
1. Develop a set of well-defined security and compliance policies.
2. Deploy the right tools to protect your system and every platform within it.
Important steps to being compliant and secure

When you set out to achieve compliance, you might meet the letter of the law while missing its spirit entirely. Consider if you want your data protected by the minimum acceptable security measures, or if you want to ensure that your data is properly protected.

The reality is achieving compliance is often not enough to truly secure your network or adequately protect data. However, if you keep your eye on the prize and aim for the best possible security protection, you attain compliance and peace of mind at the same time.

Compliance is about preventing sensitive data from being exploited or compromised. It is about taking all necessary steps to ensure only authorized users can access and view the customer information your business is entrusted with and it never falls into the wrong hands.
Summary
Here are two critical steps you can take to meet these goals:

**1. Start with well-defined security and policies.**
Your business should have established guidelines outlining proper data-handling and data-security measures, while your employees need to be aware of your policies and educated about the risks and consequences of compromising data.

You also need tools in place to help enforce those policies and security measures to monitor threats and protect data.

**2. Implement security solutions to stop phishing scams, Trojans, and other attacks.**
Use tools to identify and block both known and emerging or zero-day threats to stop malicious attacks from exposing sensitive data.

Look for integrated antivirus and antispyware solutions that provide comprehensive protection, including firewall and intrusion prevention. The best security solutions stop malicious behavior by detecting new and rapidly mutating malware, including previously unknown threats.

Achieving and maintaining compliance is no easy feat for organizations of any size, and it can seem overwhelming for small and medium businesses. But if you focus on security first—and use a state-of-the-art security solution—you’ll exceed the required compliance minimums and have a reliably secure environment, too. Symantec: the trusted partner for your small business.
Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

We have security solutions designed specifically for the unique needs of small and medium businesses. Whether you want cloud-based or on-premise security, we've got you covered.

**Cloud-based security**

Symantec Endpoint Protection.cloud™ offers comprehensive cloud-based security for your Windows® laptops, desktops, and file servers as a hosted service, helping protect your business without installing additional hardware or management software. It’s designed to safeguard your systems with advanced security technologies all managed from a single Web-based management console.

Key benefits include:

- **Advanced technologies** for antivirus, antispyware, firewall, and host intrusion prevention.
- **Automated updates** occur transparently over an Internet connection to help keep employee systems current and consistent with policies.
- **Web-based console** for administrators to access via a supported browser.
- **Proactive warning of suspicious websites** alert employees of dangerous websites and sellers so they can work online with confidence.
- **Supports service records data** about administrative activities, such as login times, policies created, and computers added.

**On-premise security**

If you prefer an on-premise security solution, consider Symantec™ Endpoint Protection Small Business Edition.

It's easy to use and protects your computers and servers with the most effective small business antivirus, antimalware technologies available in a single, integrated solution.

**A partnership you can count on**

Whether you purchase Symantec products individually or from a local Symantec partner, you can always count on protection that matches your current requirements and helps your business grow.
Three keys to cost-effective security for your small business

Learn more
Want to know more? Contact us today for a comprehensive solution for your business:

• Select a solution at the Symantec Small Business website, your online resource for recommendations, product details, and selection guides.

• Find a solution partner at the Symantec Partner website. With more than 60,000 partners worldwide, you’re sure to find one that’s right for your business.

• Request a call from a Symantec representative.