



# Managed Security Services for Small Businesses

Protecting your business cost effectively through outsourcing

# Contents

- Overview ..... 3
- The challenge of do-it-yourself security ..... 4
- MSSPs: Cost-effective approach for securing small businesses ..... 5
- Benefits of outsourcing ..... 5
- Selecting the right MSSP ..... 6
- Summary ..... 7

## Overview

Nearly every day, you hear about another security threat spreading across the Internet—Melissa, Code Red, Blaster, and Slammer, to name a few. As a small business, how vulnerable is yours? More than likely, very vulnerable.

Small businesses are connecting to the Internet in record numbers to support new market opportunities, improve employee productivity, and strengthen communications with customers, partners, and suppliers. According to Yankee Group, 70 percent of U.S. businesses with between 21 and 99 employees use broadband access, and 61 percent have mobile employees.<sup>1</sup> Likewise, 62 percent of European small businesses in France, Germany, and the U.K. surveyed by AMI-Partners have work-at-home or mobile employees or remote offices.<sup>2</sup>

The problem: The more you open your network, the more you open your business to risk. Confidential data can be exposed, customer privacy jeopardized, service availability affected, and your business reputation damaged.

Think you're not a target because of your size? Think again. If you use Microsoft software, you're in jeopardy by default. Given Microsoft's enormous market share, hackers are unleashing viruses and worms in record numbers to exploit the vulnerabilities in Microsoft Windows, Outlook, Internet Explorer, and SQL Server. These hackers want to inflict damage on a global scale, and they design their programs to spread quickly and without discrimination.

How can you mitigate your risk without taking resources away from core business activities? This white paper outlines the advantages that small businesses can gain by outsourcing security management services and provides advice on what to look for when choosing a managed security service provider.

<sup>1</sup> Mike Lauricella. "Broadband: Delivering Value and Increasing Business Productivity." The Yankee Group. July 2002

<sup>2</sup> AMI-Partners. "IT Security Opportunities Among Europe SBs—France, Germany, U.K." October 16, 2002

## The challenge of do-it-yourself security

Gartner Dataquest reports that 40 percent of small and medium-size businesses that manage their own network security will experience a successful Internet attack, and more than half of these companies won't realize they have been attacked.<sup>3</sup>

Why? Simply put, effective security can be too costly and time consuming for most small businesses to implement successfully.

Skilled security personnel are often difficult to find and cost prohibitive for small businesses. As a result, the job typically falls on a technology-savvy team member or a highly paid consultant to periodically handle all aspects of security management, including:

- Preventing emails infected with viruses, worms, and spyware from entering your network
- Ensuring that all notebook and remote desktop systems are protected so only authorized users can access network resources
- Securing communication between remote offices so it cannot be accessed or examined in transit
- Making sure that information on public servers such as Web servers is separated and protected from the business network

Because new security threats are constantly emerging, this job can become all consuming. You can't simply install an antivirus program and then forget about it. You need to ensure that your virus definitions are current and can combat the latest exploits and attacks. You must deploy security patches for your operating systems, productivity applications, and other software on all your servers, desktops, and notebook PCs as soon as they are made available by the developer. You must revise firewall rules and policies every time changes are made to your business and network. And that's just the beginning. Protecting your business from hackers, viruses, and other security threats requires continuous attention, which frequently just isn't available.

The importance of addressing these challenges in a timely fashion can't be underestimated. Consider the costs that can result from lost productivity when your network is shut down because of a virus. Irreparable damage can be done to your business reputation if confidential customer data is stolen. Add to that the possible civil and criminal penalties for non-compliance with government and industry regulations, such as the Healthcare Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, EU 95/46 EC Data Privacy Act, or any of the dozens of other regulations protecting the privacy of consumer information.

<sup>3</sup> J. Browning and J. Pescatore. "Research Note: Simple and Affordable Steps to Improve SMB Security Postures." Gartner Research. July 18, 2003

## MSSPs: Cost-effective approach for securing small business

Today's security threats are business-size neutral, leaving you with the same security challenges that large corporations face, but without the resources to handle them. Managed security service providers (MSSPs) provide an array of security services that can help small businesses close this gap.

What is an MSSP? An MSSP is a company that deploys security products as part of an outsourced managed security service. MSSPs can be value-added resellers, telecommunications providers, Internet service providers, managed service providers, or application service providers. They may only deliver security services or offer a wide range of technology-based offerings for small businesses.

Most MSSPs offer tiered levels of services that can be tailored to fit your organization's specific security needs. Under these plans, you typically pay one monthly fee for the services that you choose. These services can include:

- An evaluation of your security needs and development of a written security policy
- Hardware installation and policy implementation, such as network design and configuration and customization of firewalls and virtual private networks
- Managed security services including remote access configuration, network security protection, virus scanning, intrusion detection, anti-spam capabilities, data backup, and Web content filtering
- Monitoring, reporting, and management of alerts based on security policy and anomalies
- Automatic updates of firewall software, virus definitions, and system maintenance

In addition, many MSSPs allow you to choose whether to purchase the security hardware and software you need up front or roll the cost of the solutions into your monthly fee, allowing you to protect your business without incurring a significant capital investment.

## Benefits of outsourcing

Engaging an MSSP can produce results far superior to what small businesses can typically achieve on their own. Consider the following advantages:

### Focus on your core business

Outsourcing allows your staff to concentrate on revenue-generating business initiatives rather than infrastructure issues. Because most small businesses have limited or no IT resources on staff, managing security using your existing staff often takes the focus away from core business issues and hampers sales efforts, product delivery, and customer service.

### Reduced cost

Outsourcing security services provides you with access to a "big business" security protection at an affordable price. The expense is often more cost effective than hiring or contracting a security expert, and the consistent monthly billing rate helps ensure you obtain the security services you need without having to deal with unforeseen hassles and surprise expenses. Additionally, because MSSPs often provide an integrated, comprehensive security solution, they can help eliminate the expense of maintenance, upgrades, and add-on security solutions.

### **Benefits of 24x7 expert security staff and facilities**

If your in-house employees are usually only available during business hours, you are vulnerable when issues arise outside normal operating hours. In many cases, an MSSP can act as an around-the-clock security management department, providing 24x7 monitoring and maintenance from its facility. An MSSP also provides you with access to an Internet security expert without your business incurring the cost of hiring, training, and retaining highly skilled staff.

### **Gaining customized service**

With MSSPs, you can select the service plan that fits your organization's risk management profile and budget. As a result, you're assured exactly what you need to meet your organization's security requirements.

### **Receive up-to-date protection**

Security solutions such as firewalls, antivirus software, content filtering solutions, and virtual private networks (VPNs) are far more effective when they are maintained regularly with the latest security updates. With an MSSP, your security solutions are automatically and seamlessly updated by skilled security professionals whose only job is to ensure that your security is always current.

### **Selecting the right MSSP**

MSSPs can help you protect your business and your data. However, as with any outsourced service, how do you know that you're getting what you're paying for?

When selecting an MSSP, Check Point Software Technologies recommends that you review the following:

1. Assess the company's reputation and the expertise of its security staff. How long has the company been in business? What training and education does each person have? How do the company's security experts stay up-to-date with the latest threats? Is the MSSP familiar with security issues particular to your industry? What security products does the MSSP use as the basis of its managed security solution? Does the MSSP use a product designed for small businesses such as Check Point Safe@Office® Internet security appliances, which provide technology proven in 98 percent of the Fortune 500, but that are built for small business networks?
2. Look for MSSPs that offer a wide range of security service plans that can be customized to meet your organization's needs and deliver effortless security to your business. Can it provide you with 24x7 services if needed?
3. Confirm everything in writing. Ask for a service-level agreement that states in detail which services are included in your security plan, the procedures that will be followed in the event of an attack, how its team will respond, what the response time will be, and how it will be reported to the company. Request a confidentiality agreement that protects the security of your data. Any quality service provider should be willing to commit its promises to paper.
4. Request periodic reports on network security events so you can see that your solution is working and up-to-date. Your managed security solution should offer seamless services and periodic reports, which can be an invaluable tool in understanding the services and attack protection you get from your MSSP.

## Summary

Small and medium-size businesses aren't immune to security threats. If you use email for communications, have mobile employees or remote offices, or maintain a Web presence, your business is at risk.

Yet like many small businesses, yours likely doesn't have the internal resources to manage these threats effectively. The complexity of security issues, as well as the demands placed upon your employees, gives outsourcing these services a clear advantage. Working with a qualified MSSP can help protect your business consistently and cost effectively. As a result, your staff can focus its time on opportunities that increase your revenue, improve customer service, and ultimately grow your business.

To locate a Check Point MSSP partner in your area, visit [www.checkpoint.com/sales](http://www.checkpoint.com/sales).



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

### CHECK POINT OFFICES

#### Worldwide Headquarters

5 Ha'Solelim Street  
Tel Aviv 67897, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-575 9256  
email: [info@checkpoint.com](mailto:info@checkpoint.com)

#### U.S. Headquarters

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391 ; 650-628-2000  
Fax: 650-654-4233  
URL: <http://www.checkpoint.com>

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.