



# Meeting the Growing Security Needs of Small and Medium-Sized Enterprises

Extensible Appliances Fortify Resellers'  
SME Security Solutions

*An IDC White Paper  
Sponsored by eSoft*

Analysts: Charles Kolodgy, Roseann Day, Janet S. Waxman,  
and John Daly

## Overview

Security has become everyone's business. Most organizations are now paying careful attention to the need for better data protection and secure communications. The rise in general security awareness coincides with a groundswell of new IT security products and services that continue to evolve and expand. These products can enhance the recurring revenue stream of resellers and service providers (SPs). Advanced resellers and SPs recognize small and medium-sized enterprise (SME) customers' increasing attention to security<sup>1</sup> and are creating new business models to deliver extended security features. Some have even added a full range of security solutions and technologies to their platform or application offerings. For many of these resellers and SPs choosing to add such security capabilities, appliances offer the best value proposition.

They have selected a promising, potentially rewarding, technology. Security appliances rank among the fastest-growing segments of the worldwide IT security market. IDC estimates that worldwide customer spending on security appliances, including all channel uplift and services, will grow over the next five years to \$2.25 billion. Additional security services associated with these sales will add revenue, creating a total (product and services) market greater than \$3 billion by 2005. Value-added resellers (VARs), distributors, SPs, and integrators are viewing the large size and rapid growth of the security appliance market with great interest.

Adding security technologies to traditional application or platform solutions also allows vertical or application-focused channels and SPs to provide Internet-ready solutions to a wider range of customers. A few developments have encouraged this trend. Recent advances in easy-to-deploy security appliances are reducing expensive installation

<sup>1</sup> Security in this context refers not only to perimeter and data protection but also to secure data communications (e.g., communication via virtual private network).

costs for resellers and SPs. Plug-and-play security appliances allow solutions providers to augment their core competencies with stronger security without adding excessive overhead.

This white paper draws from IDC research on the security market and covers the following topics:

- The overall market potential for IT security in SMEs and in the branch offices of larger enterprises
- The role of resellers and SPs in the SME market
- The impact that security appliance solutions and the additional services around them exert on resellers' and SPs' relationships with customers
- A review of eSoft's channel approach, which enables resellers and SPs to extend their installed appliances' capabilities remotely

### **IDC'S APPROACH**

---

IDC developed this report using a combination of direct primary research; preexisting, wide-scale quantitative customer surveys; and security market forecasts. To understand how resellers and SPs sell, deliver, and manage security appliances, we selected three such organizations that are actively extending their solution initiatives to include these offerings. These organizations operate within the SME market and offer useful insights into that market's priorities and directions. We conducted in-depth, qualitative discussions with these organizations, exploring the particular opportunities they found most promising.

IDC also leveraged existing primary research covering security concerns and buying intentions for the SME market. We then compiled the most relevant market data and statistics, along with IDC analyst perspectives, to create a balanced view of the market opportunity in this space. This white paper reflects all of these research perspectives.

### **SECURITY AND THE SME MARKET**

---

Companies and branch/remote offices of all sizes are conducting business online. They are creating Web sites, expanding email coverage, offering remote access, and delivering increasing amounts of critical business data to employees, customers, and partners. SMEs taking advantage of these online business opportunities have streamlined business processes, reached new customers, improved customer service, expanded geographic reach, and reduced staffing costs. The benefits abound.

In large measure, the expanding reach of high-speed broadband connections (e.g., cable, digital subscriber line [DSL], and satellite)

---

Copyright © 2002 IDC. Reproduction without written permission is completely forbidden.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

*Printed on  
recycled  
materials*



*Business conditions around SMEs are often driving the change.*

has enabled these developments for SMEs and branch offices. These connections allow firms to make more information available, and, in turn, this same information then extends to other parties (e.g., customers, suppliers, and employees).

The technology alone, however, does not drive SMEs to expand their businesses online. These smaller firms traditionally focus on core business processes, remaining notoriously lean and maintaining "low overhead" when it comes to information technology (IT) infrastructure and IT staff. Instead, business conditions around them are often driving the change. For example, organizations with very few employees are implementing broadband at the behest of a larger corporate office, manufacturer, customer, or supplier. In one instance, a large insurance underwriter, striving to handle its operations more efficiently, demanded that all its independent agents upgrade their computer and communications systems to broadband technology. Likewise, small and branch offices continue to adopt broadband technology as a mechanism to expand their communications efficiencies with headquarters, partners, and customers. While focused on efficiency and speed, they highlight the need for secure data communications.

However, these same positive developments in information sharing carry risk. SMEs find that their critical business information (e.g., prices, customer lists, and supplier lists) has become more vulnerable. Increasingly, they face the following unfamiliar risk management challenges:

- **Security.** Broadband connections remain "always on," exposing SMEs to the same hackers, crackers, and mischief makers that have plagued the government and large enterprises for decades. SMEs, unlike larger enterprises, have not developed the means of effectively thwarting such attacks. They also face a maze of "new" security issues surrounding virus protection, integrity of data in transit and in storage, and control of what flows into and out of the company.
- **Administration.** Security infrastructure solutions that protect against these exposures require administration and overhead. Technologies that protect against viruses, keep data and communications secure via encryption, and control how insiders and outsiders access business data assets all require overhead and management. These security administration tasks joined with other new overhead demands, such as Web server updates, email server maintenance, and network and desktop support. The hassles of spam email or employees accessing non-work-related or inappropriate Web sites just add more overhead. All of this can appear overwhelming.

SMEs need security solutions to protect against these risks and minimize administrative overhead.

*SMEs need firewalls, VPN, virus scanning, content control business services, and more.*

## **SECURITY APPLIANCES AS AN SME SOLUTION**

Great challenges mean great opportunities. Vendors, resellers, and Internet service providers (ISPs) can address these SME problems by providing a range of Internet solutions, including security and secure data communications. Our research indicates, though, that SMEs require different solutions than those expected by larger corporations. At one level, SMEs need the same security basics that larger organizations require, such as firewall and virtual private network (VPN) capabilities. Beyond that, some SME customers are looking for the flexibility to integrate virus scanning and content control (such as URL filtering) into their environments.

Because SMEs often rely on third parties for IT functions, rather than staffing their own IT departments, they need solutions that install easily, run without much management overhead, and fit seamlessly into their current network infrastructure.

The solution of choice, and the answer to a majority of these requirements, is the security appliance. IDC defines appliances as network-enabled devices explicitly designed to provide a single dedicated service, such as a firewall, or a predefined suite of services. They run on a variety of functionally optimized and/or streamlined operating systems and chip architectures. Their nonprogrammable, preconfigured, "sealed-system" nature offers a simplicity that appeals to the SME market. Additionally, their ease of deployment and minimal cost of ownership fit the market well.

Despite their black box nature, some of these appliances do permit application upgrades via remote access. This capability provides a significant opportunity for the reseller or SP. The organization that maintains appliance access and upgrade control may activate and collect payment for additional services. For example, a standard appliance configuration for firewall and VPN may expand to include services such as URL filtering, policy management, and bandwidth management. This provides a simple upgrade path for the customer while also providing recurring revenue to the reseller or SP.

Despite the obvious fit that security appliances offer SME customers, appliance vendors must still hurdle some substantial obstacles to succeed in this sector. These customers want low prices, ease of installation, simple maintenance, and robust security and data communications. They can't afford to build nor do they want to invest in building security expertise within already slim IT departments. They are looking for help on all these fronts even as they resist premium prices.

## **SECURITY APPLIANCES AND SME CUSTOMER REQUIREMENTS**

Many excellent software-based firewalls could meet the needs of SMEs; however, these enterprises, through their VARs and SPs, are instead turning to appliances. Why? Simply put, convenience, price, extensibility, and ease of installation are the key advantages of firewall appliances. The following sections outline some of the most important factors contributing to the extraordinary growth of the firewall/VPN security appliance in the SME sector.

*Appliance Advantage: convenience, price, extensibility, and ease of installation.*

## End User/Customer Advantages

1. **Ease of installation.** SMEs cannot tolerate the standard complexities of installing and configuring software-based, server-hosted firewalls. The idea of a "connect-and-run," "no-hands" solution appeals to SMEs because they need never grapple with installing the product on an existing or new server operating environment. Therefore, they avoid the problems so often associated with ensuring version synchronization, integration with other software, and so forth.
2. **Easy, or outsourced, management.** Most firewall appliances support some level of remote management through a simple graphical user interface (GUI). In many cases, end users rely on an SP or a reseller to manage the appliance for them. Customers lack the knowledge, interest, or staff to manage these appliances internally. It is easier for them to allow their reseller or SP to maintain the system than it is to acquire the expertise to do it themselves.
3. **Remote version updating and maintenance.** Customers, resellers, and SPs may also download version updates and patches remotely. This capability helps keep firewall security current as attacks are constantly evolving.
4. **Less room for operator interaction and error.** Users and administrators often change and modify product configurations simply "because they can"; however, doing so can lead to problems. The appliance approach limits the "damage" users can do either accidentally or maliciously. These inherent limits result in fewer trouble calls and improved security.

## Reseller and SP Advantages

5. **Low overhead installation and management.** Resellers and SPs appreciate the simplicity of firewall/VPN security appliances. They find these appliances easy to install and configure at the customer location. Moreover, appliances reduce the complexity of installing and integrating security services, and they include configuration and management tools that help resellers and SPs get up to speed with minimal training. Therefore, they can get their customers up and running quickly and gain added potential service revenue.

Further, resellers can manage installed appliances from their own central, but remote, site. This remote management capability leads to service revenue increases, without the tactical and overhead burdens typically associated with servicing the client.

6. **Extensible revenue stream.** Appliances allow SPs and resellers to build on their existing relationships, providing additional features as customers require them and collecting ongoing revenue. Resellers can activate new features remotely as customers place their requests, reducing the "truck rolls" normally associated with upgrades and new feature additions. Other specific capabilities may include, for example, antivirus, URL filtering, policy

management, and bandwidth management. Customers appreciate both the added value of these features, options, and upgrades and the relatively painless means of activating them remotely. The reseller also benefits from a continued and varied revenue stream from the sale of multiple types of add-on applications, much like a printer sale generates continued revenue from printer cartridges and other print peripherals.

7. **Reduced troubleshooting time.** With remote management, resellers and SPs can limit "truck rolls," add additional services, and, in most cases, correct problems without physically going to the customer's site. The speedier trouble resolution gets the SME back in business quickly with less downtime. Likewise, resellers and SPs with limited staff can focus more time on revenue-earning activities rather than on maintenance. Remote management can also enable resellers to extend their geographic reach with less employee travel time. When the trouble involves a real problem with the product, resolution can prove quite simple. Correction involves a simple "swap-in" of a new appliance and demands no special technical expertise. The quick and simple process ensures minimal downtime.

### **Network and Security Infrastructure Integration Benefits**

8. **Integration and operating system agnosticism.** Platform OS compatibility and integration remains a problem for security product vendors and customers alike. Software security vendors face hard choices in deciding what platforms and operating systems they should support. Resellers and SPs worry about having too many products that utilize different operating systems. The firewall and VPN appliance solution avoids the entire OS conundrum by embedding a security-hardened OS that remains both inaccessible and transparent to end users. Resellers and SPs can avoid the cost and expense of extending support to a wide variety of platforms and operating systems and focus instead on added-value solutions.
9. **Synergy with high-end software solutions.** Many geographically extended enterprises use appliances in remote locations without onsite security professionals. In these situations, centralized network security staff can remotely manage security appliances as they integrate their functions with larger, centralized software-based firewalls.

### **MARKET SIZE, RESELLER/SP OPPORTUNITY**

IDC considers the following metrics when estimating security appliance opportunity in the SME market:

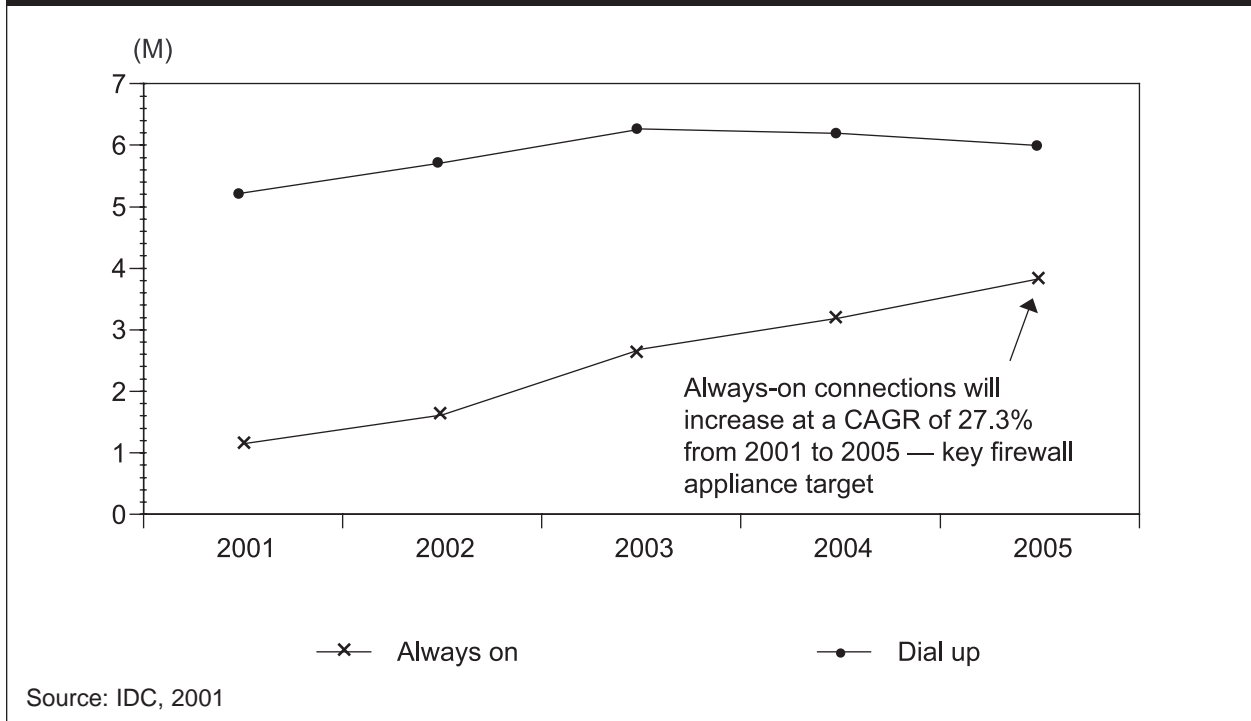
- A view of the SME market size, the total number of Internet connections within that market, and the potential for firewall appliances within that segment
- Firewall plans for that segment of the SME market most inclined to deploy high-speed connections and firewall appliances

- Appliance growth forecasts (IDC forecasts of security appliance market size and growth)

Five million U.S. businesses with fewer than 100 employees connected to the Internet in 2001.

As published in *Business Internet Access by Company Size and Bandwidth Speed, 2000–2005* (IDC #24954, July 2001), IDC estimates that 65%, or roughly 5 million, of the 7.7 million U.S. businesses with fewer than 100 employees connected to the Internet in 2001. Each of these businesses represents some level of a firewall appliance opportunity. However, of this connected group, the subset that maintains some sort of "always-on" Internet connection (e.g., leased line, fractional T1, DSL, or cable modem) represents the prime opportunity for firewall appliances. While always-on connections represent approximately only 20% of the SME Internet connections, the segment will grow rapidly from roughly 1.2 million in 2001 to almost 4 million by 2005 (see Figure 1 and Table 1).

**Figure 1: Internet Connection Types and Growth in the SME Market, 2001–2005**



**Table 1: Internet Connection Types and Growth in the SME Market, 2001–2005**

	2001	2002	2003	2004	2005	2001–2005 CAGR (%)
Always on	1.15	1.61	2.69	3.19	3.83	27
Dial up	5.23	5.71	6.27	6.20	6.00	3

Source: IDC, 2001

IDC's *Security Technology Survey* for 2001 polled these advanced SME establishments and found that 75% indicated they had installed or would install at least one firewall appliance by 2000. Another 15% indicated that they would install one in the next two years, and 10% said they didn't have plans to use a security appliance. These raw numbers seem to imply minimal demand; however, the same survey showed that over 50% of this group maintained more than three always-on connections. This finding indicates a large number of still unprotected connections and, given that the customer base has already "bought into" the solution, many additional opportunities to increase the number of appliances installed exist. Additionally, resellers can educate those less Internet-savvy customers lagging behind the market leaders.

*Market: \$1 billion now and over \$3 billion by 2005.*

Reflecting the growth in always-on connections, the overall market for firewall appliances has been growing at a robust pace. In 2000, product revenue for appliances primarily geared toward SMEs (i.e., those priced under \$5,000) totaled \$283.3 million. Further, IDC estimates that customer spending (i.e., including channel uplift and services) on such devices exceeded \$400 million in 2000. Over the next five years, the sector should grow to \$1.5 billion in revenue for manufacturers and \$2.25 billion in total end-user spending (including channel uplift and services). These figures don't take into consideration value-added services such as virus scanning and content security. Combined, the virus scanning and content security markets already exceed \$1 billion and will exceed \$3 billion by 2005.

The preceding information indicates that a great market opportunity exists for those vendors and channel partners providing security appliances for the SME marketplace.

#### **HOW THE CHANNEL DELIVERS SME SECURITY**

Concern for Internet security affects all firms. Small and large companies alike share concerns about communicating and sharing data securely over a network. SME establishments, though, as indicated earlier, will likely rely more heavily on their reseller or SP. In IDC's *Security Technology Survey*, over 44% of SMEs indicated they would outsource firewall management. Because IT security so directly affects corporate assets, more and more customers are seeking the advice, objective guidance, and implementation assistance of the organizations that sell to them.

SMEs have historically represented the largest customer segment serviced by channel partners. As SME customers' buying preferences have expanded, the channel partner's role supporting them has also evolved. Resellers in this channel, recognizing the need to expand their range of customer assistance, have focused on leveraging the expertise of other resellers through partnerships. This evolution has created an opportunity for new types of SPs that focus on specialized competencies. These SPs and resellers play a dual role in the IT ecosystems, acting largely as influencers and working with other partners for delivery and onsite service. This dual-channel approach does not work for all solutions, but it does work exceedingly well in network-edge and security-related solutions. These types of installations that

*Indirect channels lead in delivering solutions to the SME market.*

*This indirect market requires solutions-based offerings.*

*Downloading additional functionality without requiring onsite installation upgrades.*

require both the SP and the reseller to interact with the customer reveal the true benefits of the dual-channel model.

Security solutions create the perfect environment for channels to interact closely with SME customers. More customers in the SME market look to channels to help provide security consulting and services as well as applications and platform support. Resellers and SPs can deliver customer value either in a partnering environment or as a standalone, "sole-source" entity. Participation in security solution implementations also provides a unique chance for very close customer relationships. Solution-delivering companies can exert tremendous influence on the end user. Interviews indicate that many of these customers that depend on channel partners for their solutions rely heavily on these partners for additional guidance and support.

The evolving nature of this indirect market requires solutions-based offerings, not platform-based answers. Resellers, SPs, and customers alike are feeling the current economic squeeze. Channels have migrated toward leading with technology or solutions because they are no longer able to supply or have no interest in supplying hardware-dependent solutions. Technology sales drive more service and consulting opportunity and increase the partner's profit model. Security clearly is an opportunity for resellers.

#### **SOLUTION EXAMPLE: eSoft's APPLIANCES AND SOFTPAK APPLICATIONS**

---

eSoft, a software and appliance vendor, has approached the challenges faced by SMEs and branch offices with a suite of extensible products. eSoft recognized early the need for a flexible upgrade capability and extensible architecture for its appliances. The company found that as SMEs and remote/branch offices initially move business to the Internet, they tend to avoid the planning, effort, and expense required for Internet security. In the words of one reseller, "They do the minimal and get about their business." eSoft found that these customers then became very engaged and concerned once some violation of their network had occurred. At that point, they wanted security improvements installed quickly.

In response to this tendency of the SME community to request security functionality incrementally, eSoft developed a means of downloading additional functionality without requiring onsite installation upgrades. Through eSoft's SoftPak Director™ technology, resellers, SPs, and customers may select and install a variety of value-added business applications and services — called SoftPak™ applications — to install on their existing eSoft appliance. This approach offers wide flexibility in the configuration of the appliance. Customers may install a minimum configuration and then customize their appliance to reflect changes as their business needs grow. They may download and install additional functions (such as antivirus or email filtering) as needed at any time after purchasing the appliance. Although eSoft distributes the upgrades requested from the SoftPak Director distribution site, it credits the original appliance installer (i.e., reseller or SP) with the incremental sale and a portion of the subscription revenue from the newly added feature, thus providing resellers and SPs with a recurring revenue stream for SoftPak applications.

## **eSoft's InstaGate EX2™ Firewall/VPN Appliance and SoftPak Director™ Technology**

eSoft's products support SMEs and their secure Internet business applications, and the InstaGate EX2 appliance delivers firewall and VPN functions. The InstaGate EX2 has leveraged standard Intel processor technology and streamlined versions of Linux. The appliance's out-of-box functions include standard firewall functions, VPN (data communication) capabilities for linking remote sites, email hosting and management, DNS services, and intranet Web serving. Customers (or reseller/SP support services) manage these functions using a standard Web browser-based interface.

As described previously, the InstaGate EX2 appliance allows customers to use the SoftPak Director technology, a software upgrade distribution process, to download and activate new options and services as their business needs grow. The list of extended functions continues to grow and includes extended capabilities such as antivirus, network security scanning, Web content filtering, Webmail, and spam filtering software.

While the customer selects the timing and type of additional features, the reseller or SP earns a portion of the revenue associated with the sale of the new SoftPak applications.

*The reseller or SP earns a portion of the residual revenue associated with the download.*

### **ADDRESSING FUTURE MARKET ISSUES**

To stay in the lead and achieve even wider market acceptance, eSoft must hurdle a number of future obstacles. Market share and market coverage will become critical as competition to provide security to the SME community increases. eSoft must continue to leverage its solid base with resellers and SPs. These resellers offer the broader contact and distribution networks essential to SME penetration. eSoft needs to line them up as they start to provide solutions for the millions of SME establishments in the United States. Recognizing this distribution range imperative, eSoft is offering lucrative relationships to a broad network of resellers and SPs.

*Market share and market coverage will become critical.*

Likewise, eSoft must continue to keep up the very rapid pace of providing new extensions and SoftPak applications for its appliances. As security sophistication accelerates across the market, we are likely to see SMEs become more attentive to more refined security requirements such as intrusion detection, intrusion protection, and redundancy support. Even as eSoft adds capability, it must pay attention to price pressure. As the price of technology continues to decline, eSoft will experience more low-end price competition.

eSoft, and all others in this market, continue to face the challenging need for broad security education. Getting customers to understand the value of IT security technologies before they experience a major security problem may prove key to eSoft's success. Furthermore, eSoft must establish brand awareness for its products. Competitors in the security appliance space are gaining name awareness, and eSoft needs to become even more visible as an alternative. To these ends, eSoft offers a compelling economic and value proposition

for indirect partners and will continue to attract additional resellers and influencers to blanket this expanding market and deliver the technology to SMEs.

*SME establishments will look for "partners," that is, resellers, trusted suppliers.*

## **CONCLUSION**

---

The Internet continues to transform U.S. businesses, affecting large and small firms alike. eBusiness and its requirement for more and better IT security will continue to trickle down from the largest and most technologically advanced enterprises to the smallest. We have seen ample evidence of this trend in our SME surveys and qualitative primary research. However, SMEs will select, deploy, and manage their security infrastructures in ways that are fundamentally different from those of the most advanced large enterprises. SMEs will be looking for relatively inexpensive, simple, and easy-to-manage solutions to the most important of these security requirements. Security appliances, with their built-in ease of use and black box nature, fit this bill quite effectively. More importantly for resellers, we expect that SMEs will look for "partners," that is, resellers, trusted suppliers, SPs, and/or consultants, to guide them. The growth in the SME segment's need for security, coupled with its reliance on resellers and SPs to implement security, spells significant opportunity for resellers and SPs.

We recommend that resellers and SPs put security appliance competency and capability at, or near, the top of their list of priorities for product and service capabilities. If SMEs have not already started looking for appliance products, assistance, support, and management service for security, they soon will. And their needs will grow before they diminish. Our experience in this market indicates that limited use (firewalls only, for example) amplifies and expands with more eBusiness and Web activity. Progressively, email scanning, VPN tunneling, or content filtering will come into the SME segment's sights as requirements. Effectively positioned, well-connected resellers and SPs can reap dividends along the entire security maturity curve on which their SME customer journeys. The opportunities abound.

*Compelling market and business opportunity.*

eSoft provides resellers and SPs with a compelling opportunity to participate in the rapidly growing SME market. The company offers a security appliance product line that handles SME customers' most important security needs efficiently and effectively. Product installation and management require relatively minimal installation expertise or ongoing management — key elements for partners seeking to expand their solutions portfolio without the financial risks associated with extending too far beyond their core competencies. Importantly, eSoft's SoftPak applications and the SoftPak Director distribution process allow customers and resellers to selectively extend their product function without visiting the site or going through an extensive sales process. This download process supports SME customers with "on-demand" activation of features as they are needed. It also supports resellers and SPs and provides them with both immediate supplemental revenue and a deepening relationship with their clients.

In reviewing the product, the market, and the opportunity, IDC believes that resellers and SPs would be wise to explore the potential opportunity that eSoft is offering. It is an excellent time to tap into the expanded security opportunity that the Internet has created. Those companies that wait may find themselves beyond market demand for integrated security.







# IDC Worldwide Offices

## CORPORATE HEADQUARTERS

**IDC**  
5 Speen Street  
Framingham, MA 01701  
United States  
508.872.8200

## NORTH AMERICA

**IDC Canada**  
36 Toronto Street, Suite 950  
Toronto, Ontario M5C 2C5 Canada  
416.369.0033

**IDC California (Irvine)**  
18831 Von Karmen Avenue  
Suite 200  
Irvine, CA 92612  
949.250.1960

**IDC California (Mountain View)**  
2131 Landings Drive  
Mountain View, CA 94043  
650.691.0500

**IDC New Jersey**  
75 Broad Street, 2nd Floor  
Red Bank, NJ 07701  
732.842.0791

**IDC New York**  
2 Park Avenue  
Suite 1505  
New York, NY 10016  
212.726.0900

**IDC Texas**  
100 Congress Avenue  
Suite 2000  
Austin, TX 78701  
512.469.6333

**IDC Virginia**  
8304 Professional Hill Drive  
Fairfax, VA 22031  
703.280.5161

## EUROPE

**IDC Austria**  
c/o Loisel, Spiel, Zach Consulting  
Mayerhofgasse 6  
Vienna A-1040, Austria  
43.1.50.50.900

**IDC Belgium**  
Boulevard Saint Michel 47  
1040 Brussels, Belgium  
32.2.779.4604

**IDC Denmark**  
Omøgade 8  
Postbox 2609  
2100 Copenhagen, Denmark  
45.39.16.2222

**IDC Finland**  
Jarrumiehenkatu2  
FIN- 00520 Helsinki  
Finland  
358.9.8770.466

**IDC France**  
Immeuble La Fayette 2  
Place des Vosges Cedex 65  
92051 Paris la Defense 5, France  
33.1.49.04.8000

**IDC Germany**  
Nibelungenplatz 3, 11th Floor  
60318 Frankfurt, Germany  
49.69.90.50.20

**IDC Italy**  
Viale Monza, 14  
20127 Milan, Italy  
39.02.28457.1

**IDC Netherlands**  
A. Fokkerweg 1  
Amsterdam 1059 CM, Netherlands  
31.20.6692.721

**IDC Portugal**  
c/o Ponto de Convergancia SA  
Av. Antonio Serpa 36 - 9th Floor  
1050-027 Lisbon, Portugal  
351.21.796.5487

**IDC Spain**  
Ochandiano, 6  
Centro Empresarial El Plantio  
28023 Madrid, Spain  
34.91.7080007

**IDC Sweden**  
Box 1096  
Kistagangen 21  
S-164 25 Kista, Sweden  
46.8.751.0415

**IDC U.K.**  
British Standards House  
389 Chiswick High Road  
London W4 4AE United Kingdom  
44.208.987.7100

## LATIN AMERICA

**IDC Latin America**  
Regional Headquarters  
8200 NW 41 Street, Suite 300  
Miami, FL 33166  
305.267.2616

**IDC Argentina**  
Trends Consulting  
Rivadavia 413, Piso 4, Oficina 6  
C1002AAC, Buenos Aires, Argentina  
54.11.4343.8899

**IDC Brazil**  
Alameda Ribeirao Preto, 130  
Conjunto 41  
Sao Paulo, SP CEP: 01331-000 Brazil  
55.11. 3371.0000

**International Data Corp. Chile**  
Luis Thayer Ojeda 166 Piso 13  
Providencia  
Santiago, 9, Chile  
56.2.334.1826

**IDC Colombia**  
Carerra 40 105A-12  
Bogota, Colombia  
571.533.2326

**IDC Mexico**  
Select-IDC  
Av. Nuevo Leon No. 54 Desp. 501  
Col. Hipodromo Condesa  
C.P. 06100, Mexico  
525.256.1426

**IDC Venezuela**  
Calle Guaicaipuro  
Torre Alianza, 6 Piso, 6D  
El Rosal  
Caracas, Venezuela  
58.2.951.1109

## CENTRAL AND EASTERN EUROPE

**IDC CEMA**  
Central and Eastern  
European Headquarters  
Male Namesti 13  
110 00 Praha 1  
Czech Republic  
420.2.2142.3140

**IDC Croatia**  
Srednjaci 8  
1000 Zagreb  
Croatia  
385.1.3040050

**IDC Hungary**  
Nador utca 23  
5th Floor  
H-1051 Budapest, Hungary  
36.1.473.2370

**IDC Poland**  
Czapli 31A  
02-781 Warszawa, Poland  
48.22.7540518

**IDC Russia**  
Suites 341-342  
Orlikov Pereulok 5  
Moscow, Russia 107996  
7.095.975.0042

## MIDDLE EAST AND AFRICA

**IDC Middle East**  
1001 Al Ettihad Building  
Port Saeed  
P.O. Box 41856  
Dubai, United Arab Emirates  
971.4.295.2668

**IDC Israel**  
4 Gershon Street  
Tel Aviv 67017, Israel  
972.3.561.1660

**IDC South Africa**  
c/o BMI TechKnowledge  
3rd Floor  
356 Rivonia Boulevard  
P.O. Box 4603  
Rivonia 2128, South Africa  
27.11.803.6412

**IDC Turkey**  
Tevfik Erdonmez Sok. 2/1 Gul  
Apt. Kat 9D  
46 Esentepe 80280  
Istanbul, Turkey  
90.212.275.0995

## ASIA/PACIFIC

**IDC Singapore**  
Asia/Pacific Headquarters  
80 Anson Road  
#38-00 IBM Towers  
Singapore 079907  
65.226.0330

**IDC Australia**  
Level 3, 157 Walker Street  
North Sydney, NSW 2060  
Australia  
61.2.9922.5300

**IDC China**  
Room 611, Beijing Times Square  
88 West Chang'an Avenue  
Beijing 100031  
People's Republic of China  
86.10.8391.3610

**IDC Hong Kong**  
12/F, St. John's Building  
33 Garden Road  
Central, Hong Kong  
852.2530.3831

**IDC India Limited**  
Cyber House  
B-35, Sector 32, Institutional  
Gurgaon 122002  
Haryana India  
91.124.6381673

**IDC Indonesia**  
17th Floor, Tower 2  
Jakarta Stock Exchange  
Jl. Jend. Sudirman Kav. 52-53  
Jakarta 12190  
62.21.515.7759

**IDC Market Research (M) Sdn Bhd**  
Jakarta Stock Exchange Tower II  
17th Floor  
Jl. Jend. Sudirman Kav. 52-53  
Jakarta 12190  
62.21.515.7676

**IDC Japan**  
The Itoyama Tower 10F  
159-1, Samsung-Dong  
Tokyo 108-0073, Japan  
81.3.5440.3400

**IDC Korea Ltd.**  
Suite 704, Korea Trade Center  
159-1, Samsung-Dong  
Kangnam-Ku, Seoul, Korea, 135-729  
822.551.4380

**IDC Market Research (M) Sdn Bhd**  
Suite 13-03, Level 13  
Menara HLA  
3, Jalan Kia Peng  
50450 Kuala Lumpur, Malaysia  
60.3.2163.3715

**IDC New Zealand**  
Level 7, 246 Queen Street  
Auckland, New Zealand  
64.9.309.8252

**IDC Philippines**  
703-705 SEDCCO I Bldg.  
120 Rada cor. Legaspi Streets  
Legaspi Village, Makati City  
Philippines 1200  
632. 867.2288

**IDC Taiwan Ltd.**  
10F, 31 Jen-Ai Road, Sec. 4  
Taipei 106  
Taiwan, R.O.C.  
886.2.2731.7288

**IDC Thailand**  
27 AR building  
Soi Charoen Nakorn 14,  
Charoen Nakorn Rd., Klongtsonai  
Klongsan, Bangkok 10600  
Thailand  
66.02.439.4591.2

**IDC Vietnam**  
Saigon Trade Centre  
37 Ton Duc Thang Street  
Unit 1606, District-1  
Hochiminh City, Vietnam  
84.8.910.1233. 5

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and ebusiness trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, ebusiness companies and the financial community. Additional information can be found at [www.idc.com](http://www.idc.com).

IDC is a division of IDG, the world's leading IT media, research and exposition company.

01-077SOFTWA3073  
January 2002

  
*Analyze the Future*

[www.idc.com](http://www.idc.com)