



# VeriSign's Foundation in Managed Security Services

*An IDC White Paper*

Analysts: Allan Carey and Paul Johnson

As enterprises become increasingly dependent on the Internet, there is a growing trend among firms to open their network infrastructures to key stakeholders, including customers, employees, partners, and suppliers. By opening the enterprise environment to improve information flow and transaction capabilities, the inherent risks and vulnerabilities significantly increase as well. As a result, it is critical for enterprises to provide a secure environment that guarantees stakeholders the confidential exchange of information while ensuring data, message, and transaction integrity.

Similarly, as enterprises grant open access to their network resources, cyber threats grow exponentially. Whether the threats originate from inside or outside the organization, enterprises are increasingly forced to deal with a variety of potentially devastating attacks and vulnerabilities such as viruses, malicious code, Web defacement, insider abuse, and theft of intellectual property. Recent statistics released by the CERT Coordination Center at Carnegie Mellon University show that the number of vulnerabilities reported in 2001 increased 124% compared to 2000. In addition, the number of security incidents reported increased to 52,658 in 2001, a 142% increase compared to 2000 (see Figure 1).

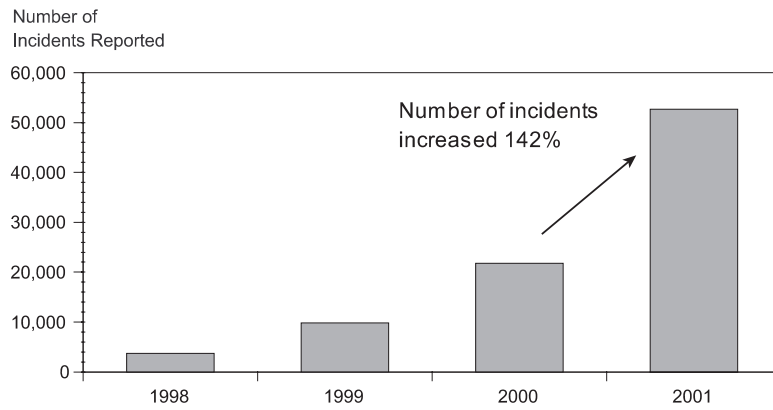
These dynamics are causing many organizations to engage third-party service providers to implement end-to-end services for security risk mitigation.

To that end, this white paper examines the following topics:

- Key trends in customer adoption of managed security services
- Factors to consider when transferring security functions to a third-party service provider
- VeriSign's Managed Security Services (MSS) offerings
- Key differentiators of VeriSign's Managed Security Services

*Sponsored by VeriSign*

**Figure 1: Information Security Incident Statistics**



Source: IDC, 2002

### **FACTORS DRIVING SECURITY SERVICES**

Companies continue to invest heavily in security hardware and software solutions to minimize business risk. IDC estimates that firms spent \$3.5 billion on security hardware and \$6.1 billion on security software solutions in 2001. Yet, many of these solutions are implemented to address an immediate challenge (e.g., a firewall deployment to allow access for legitimate or trusted traffic while keeping illegitimate or distrusted traffic out). As various security solutions are deployed, the resulting enterprise network topology becomes a complex, multivendor, multiproduct environment that is difficult to consistently manage and maintain with proper diligence and care.

For most enterprises, it is a daunting challenge to keep pace with both new and existing vulnerabilities, frequent technology platform software and hardware changes, and security policy changes that impact every function of ebusiness operations on a day-to-day basis. Significant capital investments in management technologies, facilities, and skilled personnel are required to properly and proactively secure a company's network infrastructure.

As a result, many enterprises are turning to third-party providers of managed security services. By leveraging these providers, enterprises are relying on their industry expertise and skilled resources to address the following real-world business needs and requirements:

- **Return on Investment (ROI).** Enterprises want to maximize their ROI with regard to their security resources while simultaneously reducing the total cost of ownership for their security

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



infrastructure systems. For many, this translates into rethinking their overall network and security strategies as well as their effectiveness in enabling enterprisewide business objectives.

Many enterprises struggle with the concept of measuring security ROI because of the soft metrics or "intangibles" associated with security. The biggest challenge with justifying security investments lies in the attempt to assign a dollar value to the level of security needed to adequately mitigate risk. However, with managed security services, the business case for a managed security services provider (MSSP) compared to an in-house solution is quite compelling.

IDC examines the potential cost savings associated with utilizing an external security services provider compared to managing a security solution in-house by considering the staffing requirements alone (see Table 1).

**Table 1: IDC Estimate of Staffing Requirements for 24 x 7 Security Management and Monitoring: In-House vs. MSSP**

Security Staffing Assumptions	In-house	MSSP
Number of employees per shift	1	Inclusive
Number of shifts per day	3	
Average employee annual salary**	102,500	
Employee annual security training fees	5,000	
Monthly staffing cost*	26,875	Inclusive
Average monthly MSS cost		\$3,000–\$15,000

\* Cost excludes facilities and equipment.  
 \*\* Based on salary range average provided by Lenzner Group.  
 Source: IDC, 2002

The in-house monthly staffing cost of \$26,875 is a relatively conservative estimate, taking into account one staff member per shift with three shifts per day providing 24 x 7 coverage, five days per week. More importantly, these estimates do not consider weekend shifts, additional benefits for employees, or the significant capital expenses for facilities and equipment needed to perform the security management and monitoring duties. When compared to the average monthly cost of an MSSP (typically \$3,000 to \$15,000 per month) delivering 24 x 7 x 365 protection, IDC believes that many enterprise customers can generate significant cost savings ranging from 40–70% in staffing alone.

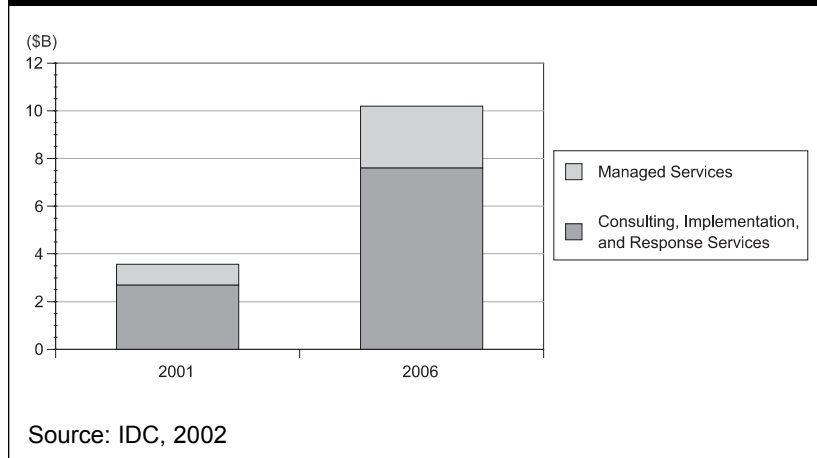
- **Security Management and Enhancement.** The challenge remains for companies to efficiently manage distributed secure Internetworks. A multitude of security products are integrated over heterogeneous platforms, which require frequent upgrades, periodic testing, and reconfigurations as newly identified vulnerabilities

arise. IDC estimates that security professionals may spend two or more hours each day collecting vulnerability information relevant to the network and its applications, resulting in as many as five new patches to be applied daily. Because effective vulnerability and security device management directly contributes to network performance, enhanced security services can lead to improved availability and reliability of business operations.

- **Consistent Security Approach.** The time and expenses associated with monitoring all external connections, internal activities, and vulnerabilities can overwhelm IT departments and corporate executives alike. As a result, security issues are often overlooked and never resolved. This leads enterprises to experience inconsistent security practices in an environment where consistency is a "must have" requirement for successful business operations and, ultimately, survival in a post 9/11 economy.
- **Shortage of Security Professionals.** Security technologies and best practices are rapidly changing to keep pace with the escalation of threats and vulnerabilities confronting the enterprise. Consequently, many in-house IT security professionals lack the core competencies or skill sets required to perform all the necessary security functions within an organization. Even more problematic, companies are challenged by the financial burden of hiring, training, and retaining skilled security professionals. According to RHI Consulting's 2002 Salary Guide, network security administrators earn between \$61,250 and \$84,750, depending on experience, skill sets, and region. The Lenzner Group estimates that an experienced security professional with risk assessment and intrusion detection skills can command a salary from \$85,000 to \$120,000. The high salaries still enjoyed by security professionals depict the true nature of the market — demand exceeds the supply.
- **Focus on Core Competencies.** IT managers are constantly seeking ways to free operational resources for higher value-added core business activities or projects. These activities leverage the IT staff's core competencies to ensure successful execution of business strategies. By shifting complicated and required security activities such as security management and monitoring to an MSSP, this enables in-house IT staff to pursue a career path with more opportunities and greater responsibilities. This allows already scarce resources to provide direct, focused support for the strategic business goals of the organization.

Given the multitude and complexity of issues confronting in-house IT security operations, the business drivers for turning to third-party providers in areas that require specialized security expertise are quite clear. For example, activities including strategic security planning, penetration testing, and cyber forensics can more easily be carried out in partnership with an information security consulting firm. IDC believes these issues are the driving forces behind the projected \$7.6 billion in U.S. spending expected for security consulting, implementation, and response services by 2006 (see Figure 2).

**Figure 2: U.S. Security Services Spending**



Furthermore, IDC expects that demand for managed security services will result in U.S. spending of \$2.6 billion in 2006, up from \$860 million in 2001. By leveraging a team of dedicated security professionals managing and monitoring networks from a hardened operations center that utilizes state-of-the-art technologies, enterprises can benefit from operational efficiencies to generate significant cost savings. The ideal situation for enterprises is to receive all of their security services from one provider — a single point of contact — with whom they can build a trusted relationship.

#### **CUSTOMER DUE DILIGENCE CHECKLIST**

As an enterprise evaluates managed security service providers, there are a number of factors to consider. IDC believes the following characteristics are important to consider during the process of evaluating a credible MSSP:

- **Commitment.** Once the enterprise has committed to security as a business-critical concern, the process begins to identify a trusted partner who can help navigate the sea of security solutions and recommend the most appropriate course of action. An MSSP should be equally dedicated to providing innovative, value-added services via a robust infrastructure, industry best practices, and highly skilled personnel. These factors reflect commitment by the MSSP, which should directly contribute to a high level of overall customer satisfaction.
- **Expertise.** Enterprise networks typically consist of complex, multivendor topologies. Enterprises look to an MSSP for security expertise because they do not possess the skills or resources to adequately manage these systems in-house. Providers should possess subject matter experts with industry expertise who understand both the technology and business issues confronting the customer.

- **Financial Stability.** One of the major concerns for customers evaluating service providers should be their overall financial stability and viability. There have been several well-publicized incidents where a provider has closed operations unexpectedly, leaving customers unprotected. The factors surrounding these business failures range from bad management and questionable accounting practices to poor strategic business planning. It is important to choose an MSSP that will be financially able to fulfill its contractual commitments.
- **Breadth of Services.** Security is a multifaceted issue that cannot be addressed with technology alone. Enterprises must take a holistic approach by incorporating people, processes, and technology to establish a comprehensive risk mitigation program, with a heavy emphasis on people and process in the context of proactive management. A successful program must continuously assess, detect, protect, and respond against potential network vulnerabilities. In addition, with respect to detection and protection capabilities, an MSSP should exhibit the necessary and relevant industry, business strategy, technical, and educational competencies to provide end-to-end services that fully address all of a customer's evolving security needs.
- **Scalability.** As businesses mature, their IT requirements change and grow accordingly. Companies may require additional security services to strategically plan for this growth, such as developing a technology migration path to support operational expansion. Enterprises should select a vendor with services that can easily scale to meet the new business requirements.
- **Service Level Agreements (SLAs).** SLAs are the benchmark by which most customers evaluate their service provider and internally justify the value received from the managed services to executive management. The vendor selection process should include two key criteria:
  - A service provider that offers consultative advice about choosing the appropriate service package
  - A service provider that commits to backing its SLAs with meaningful penalties when metrics are not met

## **VERISIGN'S SECURITY OFFERINGS**

---

VeriSign is a \$1 billion publicly traded company (NASDAQ: VRSN) headquartered in Mountain View, California. Since 1995, the company has invested more than \$400 million in infrastructure buildout and improvements, establishing VeriSign as a global provider of digital trust and managed Internet and security services. VeriSign's digital trust services, including authentication and payment services, are provided via its global infrastructure that manages more than 6 billion communications and transactions per day. VeriSign's managed Internet services, including registrar, global registry, and managed domain name services provide issuance, management, and transfer capabilities of top-level dot-com, dot-net, and dot-org Web domains.

The company also has relationships with 48 affiliates worldwide that provide trust services under licensed, co-branded agreements employing VeriSign technology and business practices.

### **Security Consulting Services**

The increasing complexity of today's global business environment, heterogeneous IT infrastructures, and cyber threats has increased demand for comprehensive security consulting services. VeriSign's Security Consulting services incorporate a broad range of solutions — including strategic consulting, design and architecture, implementation, and customized education and training — that help organizations effectively assess, protect against, detect, and respond to security threats from inside or outside the enterprise.

By utilizing the experience and knowledge of more than 300 globally deployed security and networking consultants, these offerings enable VeriSign to mitigate customers' security risks resulting from open, Internet-connected networks.

### **VeriSign Managed Security Services**

To successfully address customers' evolving security requirements, VeriSign continues to bolster its portfolio of security consulting services with a more robust solution set. VeriSign's Managed Security Services (MSS) have been developed as a natural extension of the company's foundation in providing managed registry, domain name (DNS), and Public Key Infrastructure (PKI) services. In addition, VeriSign's MSS portfolio rounds out an end-to-end customer solution that augments previously established network and security infrastructures built by VeriSign for its customers.

Table 2 defines the services available within VeriSign's Managed Security Services offering.

In addition, VeriSign operates its Managed Security Services infrastructure 24 x 7 x 365 from a redundant system of network operations centers (NOCs) dispersed throughout the world. More than 120 technical professionals, averaging 10 years of industry experience, manage and monitor customers' network activity from these NOCs. VeriSign's technical professionals combined hold more than 364 industry (e.g., CISSP) and vendor (e.g., Check Point and Cisco) certifications.

## **VERISIGN'S MANAGED SECURITY SERVICES KEY DIFFERENTIATORS**

---

### **Strengths**

In the highly fragmented MSSP market, each competitor provides its own set of services and capabilities, making it difficult for enterprises to scrutinize the marketing and sales rhetoric to determine the relative strengths and services that differentiate each competitor. IDC has identified the following five strengths that distinguish VeriSign in the MSSP market:

**Table 2: VeriSign's Managed Security Services Portfolio**

Service	Description
Firewall	Single or high-availability configurations; firewall policy and rule base creation; firewall logs customized and maintained to capture service level actions and events; alert monitoring; statistics on firewall performance and security configuration
Intrusion Detection	Monitored detection of distributed denial of service attacks, including IP spoofing and port scanning, among others; automated alerts and trouble ticket generation for critical alerts; customer notification of critical alerts
Virtual Private Network (VPN)	Single or high-availability site-to-site and client-to-site configurations; maintenance of IPsec compliant tunnels; performance statistics, certificate/authentication integration; client support
Authentication	Strong, two-factor and certificate (X.509) based; key and certificate database creation and maintenance
DNS/IP	Fully redundant DNS implementation; maintenance and update of DNS zone files and IP address allocation; auditing and reporting statistics
PKI/Digital Certificates	PKI infrastructure creation and maintenance; managed certification process includes registration, naming, appropriate applicant issuance, revocation, suspension, repository maintenance and audit-trail generation

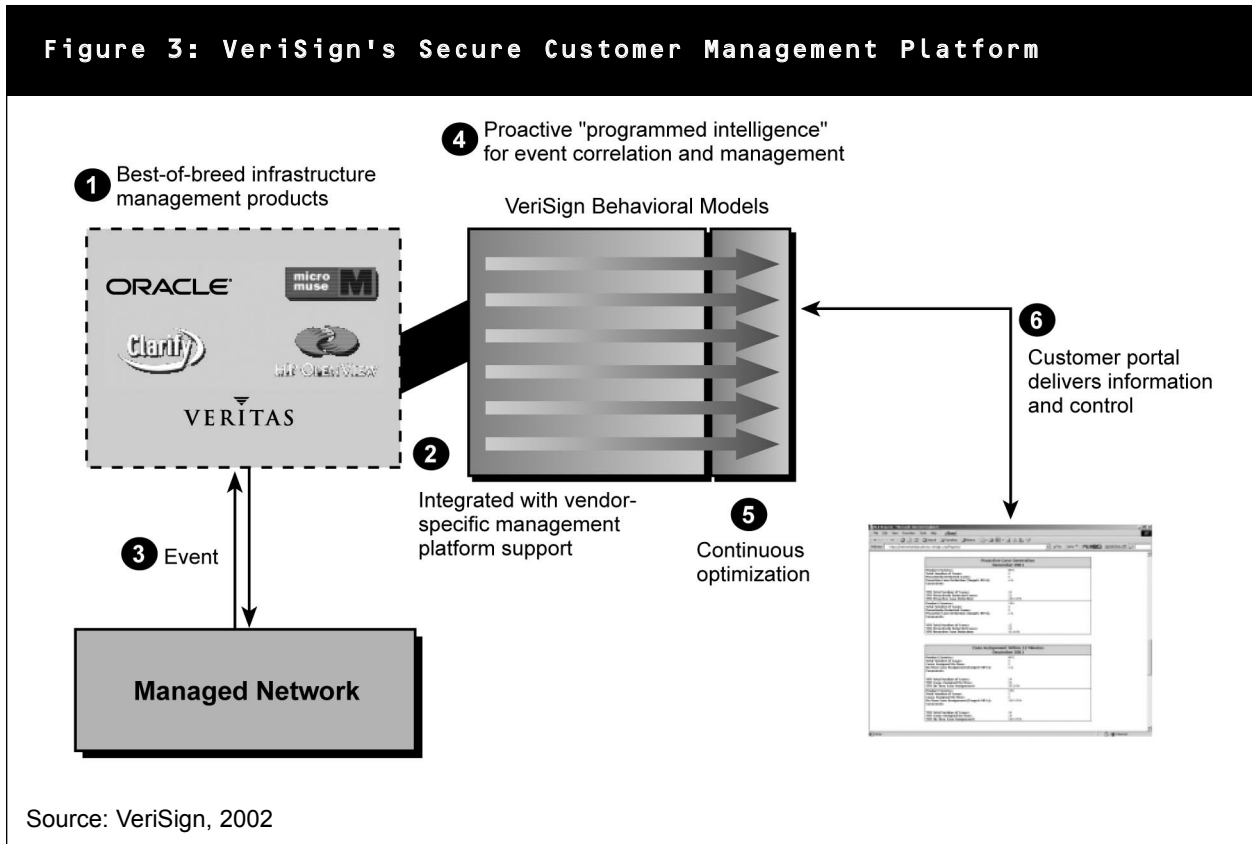
Source: IDC, 2002

- **End-to-End Capabilities.** With network and security assessments, architecture design capabilities, as well as management and monitoring services, VeriSign's portfolio of security consulting and managed security services offers customers various points of entry to engage the company as a trusted advisor on any aspect of life-cycle security design, implementation, and management.
- **Event Correlation.** The VeriSign Correlation Engine is seamlessly integrated into VeriSign's Secure Customer Management platform architecture and serves as a key enabling technology that provides event filtering and anomaly detection. The correlation engine is incorporated into each of VeriSign's managed security service offerings at no additional cost.
- **Proactive Management.** VeriSign continues to build upon its growing repository of behavioral event models. Leveraging a customized version of Veritas' NerveCenter, tightly integrated with monitoring tools including MicroMuse Netcool and HP OpenView, these models are developed to complement the correlation engine and provide a more holistic view of threat and

anomaly activity. To date, the repository contains over 80 discrete behavioral triggers that allow for automated, proactive management of customer environments. This feature allows VeriSign to detect problems before they become outages.

In addition, the distributed nature of the underlying architecture further enables VeriSign's MSS to easily scale as the customer's enterprise grows and requires increased management loads. Further illustrating the services' scalability, 1,800 trouble tickets were proactively generated in 2001, which represented 96% of the overall total tickets generated and enabled VeriSign to meet and exceed SLA requirements (95%) for proactive management. During the first quarter of 2002, the number of trouble tickets managed increased by 455%; yet, the service improved its SLA hit rate to 98%.

VeriSign's secure, proactive, management platform architecture is outlined in Figure 3. The company committed \$20 million to integrate the various management technologies at Step 1, which provide the foundation of the scalable, automated nature of VeriSign's MSS offerings.



- **Web-Based Customer Portal.** VeriSign's Customer Care Web Portal provides customers with access to customizable reports to address the various needs of business constituents at all levels of the organization. The reports include detailed information such as

the status of pending services delivery and service performance against SLA metrics. Customers also have the ability to request changes, ask questions, or escalate an event as well as view current and historical management activity via the Web portal.

- **Service Level Agreements (SLAs).** Each managed service is backed by guaranteed SLAs with financial penalties for any missed SLA metric. Using the Customer Care Web Portal, VeriSign proactively reports against the SLAs on a monthly basis, with credits for failing to meet service levels generated automatically and proactively.

The targeted MSS metrics that are a component of every VeriSign SLA include:

- 95% proactive monitoring to identify a possible trouble condition
- 90% case assignment to a security engineer within 15 minutes of receipt of trouble
- 100% customer notification of status within 30 minutes of receipt
- 90% of all trouble case tickets closed within six hours

Over the past 2 1/2 years, VeriSign has consistently exceeded targets and customer expectations for each metric category listed above.

### **Challenges Moving Forward**

While VeriSign boasts a rapidly growing customer base and revenue stream, the company still faces challenges as it competes in the highly competitive managed security services market.

First, it competes against a number of other established players in the marketplace. As a result, VeriSign should leverage its brand recognition and global capabilities, while continuing to focus on successful engagements within its Global 2000 customer base.

Second, the current economic climate is forcing many potential customers to consider the financial backing of its managed service provider. As a result, VeriSign must continue its pattern of demonstrating consistent year-over-year revenue growth and improved cash flows to alleviate any customer concerns.

Finally, given the mission-critical nature of security services, enterprises are reluctant to allow service providers uncontrolled, open access to their networks and confidential information. VeriSign has an opportunity to build upon its track record of having created a trusted transaction environment for more than 4,400 enterprise customers. The company must continue to demonstrate that it is capable of providing highly reliable, secure, and scalable managed security services while simultaneously delivering the highest level of customer service and providing the appropriate level of customer-desired control.

## **CONCLUSION**

---

Ultimately, managed security services is a trust business. IDC believes MSSPs must demonstrate their competencies in security and their ability to deliver a high quality of service in order to win a customer's confidence and trust. In addition, IDC believes a robust, end-to-end solution approach to security risk management most effectively addresses the needs of enterprise customers. VeriSign's extension of its Security Services portfolio into Managed Security Services strategically positions the company as a full-service security solutions provider capable of addressing the expanding, immediate, and future needs of both its enterprise customers and the security marketplace overall.

# 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 Benelux (Belgium)**  
Boulevard Saint Michel 47  
1040 Brussels, Belgium  
32.2.737.76.02

**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  
Amsterdam1059 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**  
Fortuny 18, Planta 5  
28010 — Madrid  
Spain  
34.91.787.2150

**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 200  
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  
65.6226.0330

**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  
3-7-18 Mita, Minato-ku  
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.

02C3333SERVIC3333  
May 2002



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