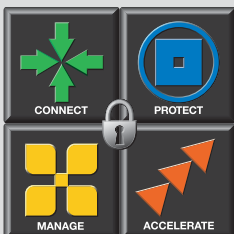


Information Security as a Business Enabler

**Deloitte
& Touche**

In this Document

- 1 Introduction
- 2 Leveraging the “Network Economy”
- 3 Information Security Challenges
- 4 Corporate Security Challenges
- 5 The Role of the Executive Officers
- 6 The Complete Security Solution—SVN and IPOV
- 7 A Model for Success
- 8 Access Control
- 9 Management
- 10 Environment Access
- 11 Infrastructure Integrity
- 12 Conclusion



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Deloitte
& Touche

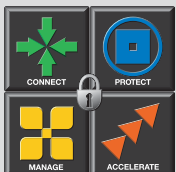
INTRODUCTION

The traditional view of information security in many companies is often a tactical one: invest where necessary to protect corporate information assets. It's perceived in much the same way as buying insurance—paying for it is cheaper than the alternative should disaster strike. With the increase of business globalization and the dawning of the 21st century Network Economy¹, however, an opportunity exists for business leaders to leverage effective information security as a business enabler, and even as a competitive tool. By establishing the policies, processes and technologies needed to create a secure information infrastructure, businesses can now have the confidence to share information with global peers, customers, partners and suppliers. This trusted network of information exchange is the foundation for a higher level of new services, an improved customer experience, and offers organizational productivity gains that translate to measurable operational savings, while decreasing time to market.

Check Point Software Technologies Ltd.— the worldwide leader in security, provides the security businesses need to connect, protect, manage and accelerate their information systems. Check Point's Secure Virtual Network (SVN™) architecture provides a framework for connecting all of an organization's users, applications, networks and systems in a secure, manageable environment. As a pioneer in information security technology, Check Point has created the SVN architecture to deliver best-in-class connectivity and security solutions, with a focus on industry standards and vendor interoperability that allows clients to integrate Check Point solutions into any client environment.

Deloitte Touche Tohmatsu is one of the world's leading professional services organizations, delivering world-class assurance and advisory, tax and consulting services through its national practices. As a recognized leader in information security consulting, Deloitte & Touche Security Services has more than 800 professionals in 35 cities worldwide who can help clients make the right choices. Their place as trusted advisors for over 140 years has been earned by understanding the intricacies of how people, process and technology are dependent upon each other.

Check Point and Deloitte & Touche Security Services have realized, through their extensive client relationships, that the general industry is desperately seeking a comprehensive security strategy—one that combines technology and organizational processes in an effort to obtain a desired level of electronic asset protection. For this reason, Check Point and Deloitte & Touche have partnered to provide clients with unrivaled market experience, state-of-the-art security solutions and a cost-effective budget model. Together the alliance offers sophisticated security service products while promoting best practices for deploying, integrating and assessing security solutions.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Deloitte
& Touche

Leveraging the “Network Economy”

Ubiquitous computing power and affordable telecommunications access have created an opportunity for global webs of business relationships enabled by massive connectivity. Deloitte & Touche calls this the “Network Economy.” The “Network Economy” is one of the single strongest drivers of business transformation, as global companies refocus their efforts on their true core competencies and reach out to other global entities to create interdependent “best in world” relationships. Companies looking for stronger operational efficiencies and competitive advantage can capitalize on this mass interconnectivity by focusing on those core capabilities, looking at what makes their company unique, and establishing business partnerships with other premier suppliers of the goods and services that are necessary to complete their customer offerings. The end result is an interconnected “virtual” corporation that is the combination of many business partners serving customers as one company. The key to building and managing these global relationships is the effective exchange and management of information across a secure global information infrastructure. The “Network Economy” is based upon the effective gathering, exchange and utilization of information from customers, peers, suppliers, regulators and lawmakers and even competitors. A Secure Virtual Network (SVN) connecting all of these entities, and the business practices and policies that surround this information exchange are vital to business success in the “Network Economy”.

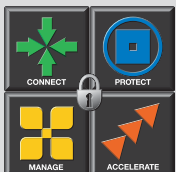
Information Security Challenges

With the ever-increasing sophistication of the hacking community, global electronic terrorism and corporate espionage, the need for effective and timely security measures has taken center stage in protecting information assets within the “Network Economy”. With this demand the technology industry has responded with a myriad of solutions including faster firewalls, effective intrusion detection tools and stronger authentication methods. Many technology companies have rushed to meet the opportunity this increased interest has provided. Clients, however, have been left with the daunting task of sifting through the many options and vendor claims, positioning an effective ROI proposition and integrating a potentially complex solution into their current infrastructure.

Experience has shown that success or failure in designing and deploying an effective IT security solution rests on the skills and willingness of multiple parties to form an effective team. An effective and secure IT solution must:

- Meet the current requirements of an enterprise
- Deliver the benefits specified by vendors
- Integrate well within existing IT systems

Instances where implementations have not taken these success factors into account have resulted in failure. If eBusiness is to grow and thrive, the public *must* trust IT security products and services. IT products and services provide the first, second and third lines of defense, ensuring the security and simultaneous growth of the Internet-based economy. Hence, security solutions become a critical success factor and a direct enabler of many, if not all, Internet-oriented business solutions.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

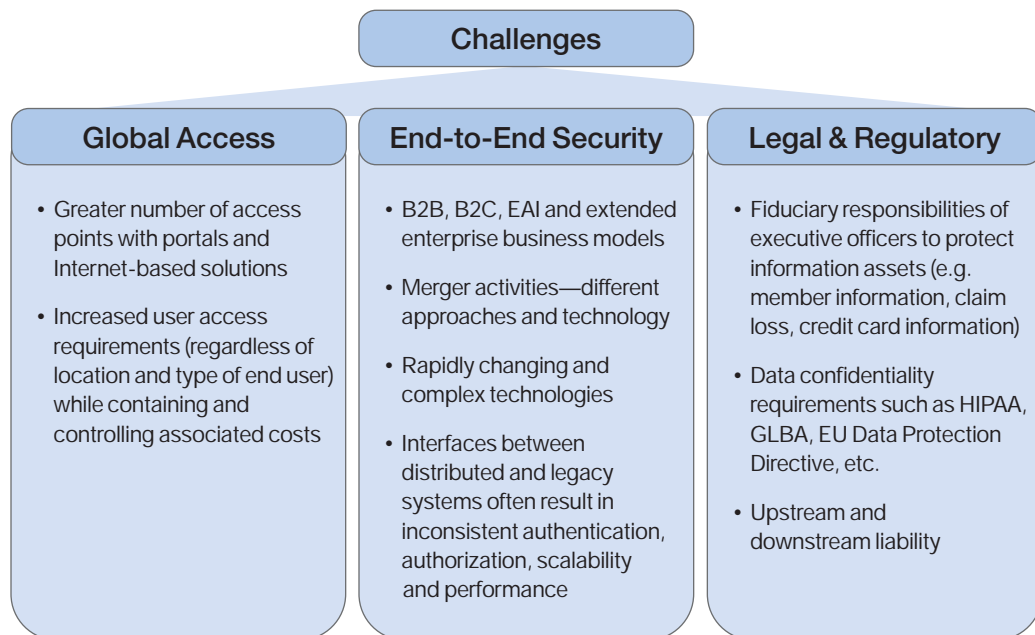
Deloitte
& Touche

Corporate Security Challenges

As companies search for better ways to connect to their customers and business partners, they face change in the way they do business, and in the IT systems that support their business processes and communications. IT management's expectations in these organizations are clear:

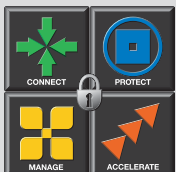
- Mitigate Risk
- Enhance Business Productivity
- Reduce Cost
- Streamline Application Development/Integration

However, organizations are struggling to balance how to provide cost effective security while meeting on-going business challenges:



Meeting these challenges means conquering an apparent paradox—access with accountability. Corporations wishing to capitalize on the financial benefits of eBusiness must learn to do business on the Internet. Doing business on the Internet means utilizing a public network that, on its own, is untrusted.

An effective information security strategy is the key to meeting these business challenges. By treating security as an enabler of manageable, accountable and scalable access, not just a traffic cop, security becomes the catalyst for safe and open information exchange. From this perspective, security is no longer just a straight cost but rather an investment in business growth and development. Security becomes the vehicle by which new business opportunities are realized and enables the next-generation of eBusiness—an environment where business practices and applications can be shared in a model of trust and accountability.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Deloitte
& Touche

The Role of the Executive Officers

Once an information security strategy has been developed, the next challenge is effectively managing the risks associated with implementation and operation. Security implementation challenges are predominantly organizational and cultural:

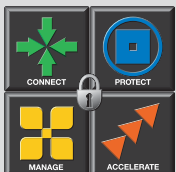
Most Enterprise Security Programs and Initiatives Fail Due to Lack of Business Unit and/or Executive Buy-In

- Lack of demonstrated ROI
- Poor definition of success
- No real business alignment
- No long-term strategy to decrease the level of overall security risk and exposure
- No real standardization
- No framework within which to design and deploy solutions for new problems
- Technically led IT-based security projects
- Perceived loss of agility (i.e., flexibility and tailoring to meet unique business needs)
- Shifting responsibility without accountability:
 - Budget and cost management
 - Security and risk management
- Low prioritization of security as compared to business initiatives
- Lack of appreciation for the importance of security in today's enterprise
- Disconnected between enterprise and business unit goals
- Security management organizational alignment
- Immaturity of technology solutions

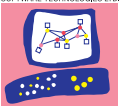
Successful information security implementation requires involvement at all levels of an organization, particularly the executive management level, because of the impact to business processes and policies and the value security has as a business enabler. Having alignment towards the goals of a business and full organizational support best minimizes security implementation risk. This support begins with top-level management and should be treated as a key strategic business initiative in order to be successful and deliver a full return on investment.

The Complete Security Solution— SVN and IPOV

Security implementations that only encompass IT-driven technology selections without the business best practices that complement them are incomplete and usually fail to deliver full value to the organization, in addition to being more vulnerable to "social engineering"² and other security attacks. It is for this reason that Deloitte & Touche and Check Point have partnered to deliver complete security solutions to their clients. Companies need a robust, comprehensive security solution—only protecting the perimeter is not enough.



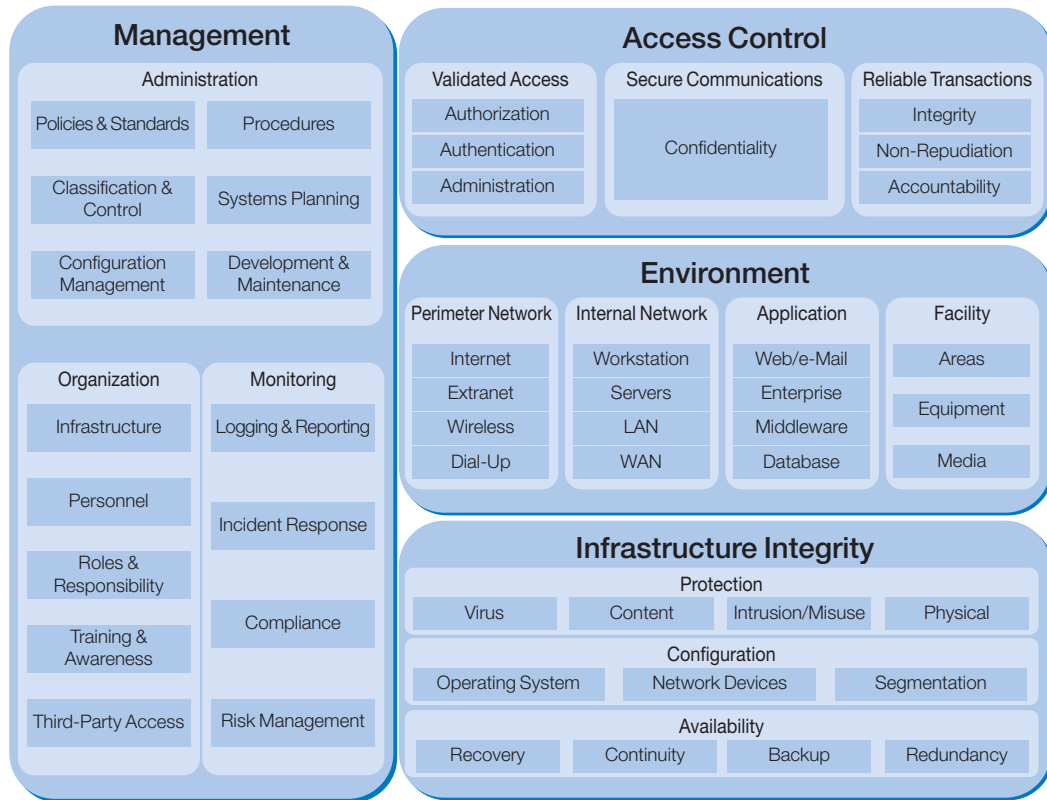
Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Deloitte & Touche

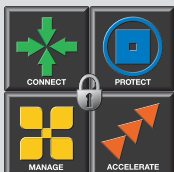
Deloitte & Touche approaches this challenge from its Infrastructure Point of View³ (IPOV):



Security by IPOV creates the essential administrative and technical prerequisites that an enterprise needs to address before it can deploy secure business applications. IPOV is a framework for Deloitte & Touche Security Services to ensure that a company’s resources are protected and enterprise-wide security awareness is maintained. These services do so by enforcing the company’s established security governance while taking into consideration best security practices.

Deloitte & Touche employs IPOV in system integration and consulting engagements. It helps Deloitte & Touche to design and implement infrastructures that enable clients to create a cost-effective management infrastructure that meets the objectives of:

- Security
- Manageability
- Scalability
- Performance
- Reliability
- Flexibility



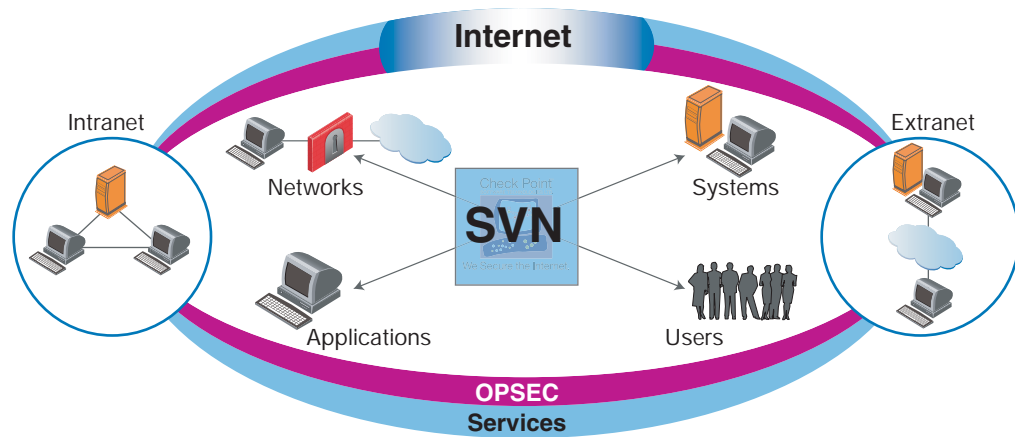


We Secure the Internet.

**Deloitte
& Touche**

The Check Point Secure Virtual Network (SVN) solution set aligns precisely with this model by offering a comprehensive architecture that can connect and protect all elements of eBusiness: networks, systems, applications and users. To complement Check Point's core products, SVN leverages the open systems benefits of Check Point's Open Platform for Security (OPSEC), the industry's leading, open, multi-vendor framework for security technology interoperability.

With SVN, every aspect of a client's information network is secured—Internet, extranet and intranet—ensuring data is protected regardless of where it resides or how it is being exchanged.



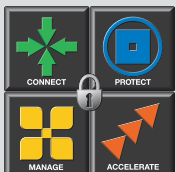
A Model for Success

The IPOV model provides a valuable framework for creating an effective business security strategy. The SVN architecture addresses the key infrastructure needs of a comprehensive security strategy. By encompassing all key technology areas, as well as the business functions that surround them, clients can ensure they develop a complete strategy for implementing a trusted information infrastructure.

Access Control

In the IPOV model, access control encompasses the ability to verify identity, grant access to authorized resources and provide accounting for access activity and administrative changes. Access control also includes the need to maintain secure communications and data integrity. With corporations increasingly turning to outsourcing business models, electronic supply chain management strategies and granting customers more direct purchasing and account management options, a thoroughly defined strategy for access control is paramount.

Security policies must have the intelligence to enforce security based on specific applications or users, and should never rely solely upon information contained in IP packet headers, as is done with simple packet filtering. Check Point meets this challenge with very granular access control that allows security administrators to map authorized users to specific applications, and even specific areas of individual servers, without exposing other confidential areas of the infrastructure. The business benefit of this capability is greater security and the confidence that the connection to customers and business partners is a trusted, accountable information exchange.



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

**Deloitte
& Touche**

Another key concern when granting third-party access to trusted internal systems is the ability to verify the integrity of the systems being used for access. In a model where a company does not directly own all the systems being used to access their applications and corporate data, a methodology for verifying that those systems have not been compromised by a known virus or malicious modification of system software is critical to minimizing security risk. Check Point products such as VPN-1® SecureClient™ offer the ability to enforce security policy down to the individual desktop or access device, including PDA's and cellular phones. By verifying security and system integrity to this level, the integrity of the information infrastructure is maintained.

Management

The management domain represents the core of defining, managing and monitoring a Secure Virtual Network. It is where the intersection of business practice and technology is most apparent, and the area where the value of the Deloitte & Touche and Check Point partnership is most obvious. The best practices and methodologies developed by Deloitte & Touche to help clients define global security policy can then be enforced through Check Point's SVN security architecture.

The key to realizing an organization's security strategy and maximizing IT resources is effective management of the security infrastructure. Check Point's SmartCenter Pro™ and Provider-1® management solutions address this challenge by providing security managers with the ability to truly manage a distributed security environment from a central location. This capability translates to a savings in administrative time and results in a more secure information infrastructure by minimizing individual entries and security policy changes, and thereby reducing the chances for human error.

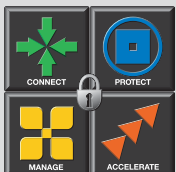
One of the top security risks in any infrastructure deployment is the improper configuration of key security components. Check Point provides a unique architectural approach to reducing this risk through its integration of firewall and VPN functionality into a single platform. By integrating these key components into a single solution and integrating the configuration and management under one interface, the opportunities for human error are greatly mitigated, and the overall complexity of managing the SVN is reduced.

Environment Access

Deloitte & Touche's IPOV defines this domain as components and technologies that permit data access to various well-defined levels: to the perimeter or internal networks, to applications and to physical facilities. A fully comprehensive security solution must address each of these areas.

In order to offer robust protection for information resources at all points within the infrastructure, a strategy for protecting all components of the information chain is required. Check Point's SVN solution set has addressed this need with products that protect not only the perimeter (whether at the Internet point-of-presence, remote access or extranet connection), but also internal networks and applications servers that run a client's business. In fact, this protection can be extended to the individual workstations and users that access company resources, to offer the greatest level of control and accounting. This comprehensive security approach provides end-to-end security, regardless of where communications originate or end.

Studies have also shown that the majority of recently publicized security breaches were the result of an "inside job." Therefore, simply protecting the perimeter is not enough. Installing a firewall at the edge of a company's network is a component of a secure information infrastructure, but not a complete solution. An effective security architecture must offer protection at all levels of the infrastructure, including desktops, applications and internal networks. Check Point's SVN architecture was created to mitigate these risks.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Deloitte
& Touche

There are also numerous cases where the absence of well-defined procedures can leave internal resources exposed. Having the appropriate procedures for revoking access for a departing employee or verifying identity before creating new accounts are just two examples. For this reason, the security policies and procedures that Deloitte & Touche can help their clients develop and implement are a mandatory complement to security technology.

Infrastructure Integrity

Infrastructure integrity refers to the processes and mechanisms enabling the protection of infrastructure, as well as its ongoing availability. Security is not a static state, but rather a dynamic process that must be continually monitored, managed and improved. Clients need the tools and processes for adapting to new threats, and scaling their secure information infrastructure to meet new business needs.

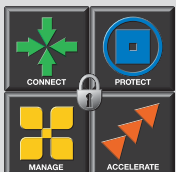
Check Point's SVN solutions offer a counter to the pure "security in a box" approaches being offered by other vendors. Given the ever-changing nature of security threats, Check Point has chosen to continue focusing on software development vs. hardware R&D. This strategy gives clients the choice of the hardware that meets their IT and security standards, with the ability to deploy the Check Point software solutions on a choice of hardware platforms offering value-add options such as load-balancing, high availability and enhanced management visibility. This approach allows Check Point to focus on development efforts that provide the best security software, giving clients multiple options for deployment platforms. This offers clients a unique benefit for this security space—choice.

Clients also need the ability to incorporate "best of breed" solutions that reach beyond the firewall/VPN technology, which can be easily integrated with their existing security environment. Check Point's SVN addresses the need for vendor interoperability with its OPSEC alliance program. Through this program, more than 325 technology partners have joined the alliance to ensure that their products seamlessly integrate with Check Point's SVN solutions. This "open systems" approach offers the greatest potential for having the best solution to new threats and the most flexibility in responding to changing business requirements.

Deloitte & Touche offers a range of services in this domain that can aid clients in integrating the Check Point core technologies with the appropriate OPSEC partner technologies to provide the most comprehensive and effective security infrastructure. These services include:

- Network Controls Security Assessment
- Network Security Architecture and Design
- Network Controls Technology Evaluation and Selection
- Network Controls Policy and Standards Development
- Network Controls Solution Design
- Network Controls Solution Implementation
- Network Controls Assurance and Compliance
- Enterprise Security Architecture Solutions

For more information regarding Check Point solutions and/or Deloitte & Touche services, please go to www.checkpoint.com and www.deloitte.ca.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Deloitte
& Touche

Conclusion

The Internet allows for global communication, but with it comes inherent risks. Check Point's SVN architecture provides a scalable, integrated framework for deploying and managing Internet security. It is designed to meet the security requirements for today's eBusiness and provide a solid foundation for emerging security needs. Organizations must have a security solution that is interoperable with third party, best-of-breed products and services to integrate seamlessly into one security solution at the policy level. The Check Point SVN architecture with their Open Platform for Security (OPSEC) alliance program delivers an open, extensible, standards-based security framework

Deloitte & Touche's Infrastructure Point-of-View (IPOV) methodology is designed to assist clients in developing and implementing a robust, holistic enterprise security program. This approach is required to allow organizations to shift from an IT-centric to a business-centric security process in order to more effectively manage risk. Benefits of such a program are self-evident:

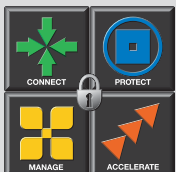
- Links all necessary organizational, technical, administrative and physical security controls to a strategic combination of business drivers, legal requirements, threat scenarios and design
- Ensures they are operationally integrated with the overall IT architecture, business processes and business culture

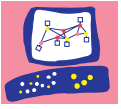
Deloitte & Touche's IPOV and Check Point's SVN are more than compatible—they should be applied together to create the comprehensive security strategies that enable business growth and development in the global marketplace.

¹ Deloitte & Touche defines the Network Economy as the business environment created by massive global communications interconnectivity and the resulting interdependent business relationships.

² Social engineering is the practice of masquerading as a business employee, customer, or supplier in an attempt to get a company to disclose confidential information or provide access to secured systems.

³ Deloitte & Touche's *IPOV* is a complex model, but it makes up only one element of an all-encompassing Deloitte & Touche proprietary methodology, "Security Architecture Point of Views". The present white paper does not attempt to cover this methodology.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

About Check Point Software Technologies

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. The company's Secure Virtual Network (SVN) architecture provides the VPN and security infrastructure that uniquely enables secure and reliable Internet communications. SVN solutions, as delivered in the company's Next Generation product family, secure business communications and resources for corporate networks, remote employees, branch offices and partner extranets. Extending the power of SVN is Check Point's Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 325 leading companies. Check Point solutions are sold, integrated and serviced by a network of 2,500 certified partners in 149 countries. For more information, please call us at (800) 429-4391 or (650) 628-2000 or visit us on the Web at <http://www.checkpoint.com> or at <http://www.opsec.com>.

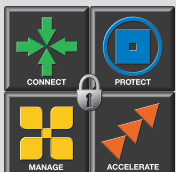
CHECK POINT OFFICES:

International Headquarters:

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: 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 Check Point Software Technologies Ltd. All rights reserved. Check Point, the Check Point logo, FireWall-1, FireWall-1 SecureServer, FloodGate-1, INSPECT, IQ Engine, MetalInfo, Meta IP, MultiGate, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SVN, UAM, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Appliance, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 SecureClient™, VPN-1 SecuRemote, VPN-1 SecureServer, and ConnectControl are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. 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 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications. P/N 500796