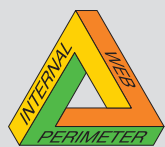


# Build Your Security Infrastructure With Best-of-Breed Products From OPSEC

## In this Document

- 1 Introducing a Solution to Your Security Challenges
- 2 Building a Comprehensive Security Solution
- 3 Framework for Integrated Security Management
- 4 OPSEC Integration Points
- 5 Benefits of the Check Point OPSEC Framework



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## Introducing a Solution to Your Security Challenges

Enterprises are challenged to open their networks over the Internet to customers and suppliers seeking real-time access to business critical data. However, without proper security, every part of the network is at risk from unauthorized activity from hackers, competitors and even employees. In the past, security threats were easily traceable and contained by a single point product. In recent years, however, security threats have become more complex and combine viruses, hacking and denial of service attacks. Recent threats like CodeRed and Nimda were able to quickly propagate throughout networks and cause billions of dollars in damages. No single product or vendor can eradicate threats caused by these combined attacks. Enterprises, therefore, must deploy multiple security products to effectively manage their security goals in today's highly competitive business environment:

- Protect the network against Perimeter, Internal and Web-based attacks and threats
- Respond to attacks and intrusions in real time
- Provide selective network and application access to partners through extranets
- Deploy a single security policy across all security applications
- Ensure performance, reliability and availability without compromising security
- Centrally administer comprehensive security policies across the entire network

## Building a Comprehensive Security Solution

### Firewalls—The First Line of Defense

Network security starts with protecting the perimeter of the network. Firewalls are installed at the gateway of the enterprise's network and any subnets that need additional security. Check Point's VPN-1®/ FireWall-1® is the first layer of a multi-layer security architecture primarily acting as an access control device. FireWall-1 uses Stateful Inspection technology ([http://www.checkpoint.com/products/downloads/Stateful\\_Inspection.pdf](http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf)) to inspect traffic and make intelligent access decisions. Once network traffic is authorized by the firewall, other security applications are invoked for subsequent levels of protection.

### Intrusion Detection Systems

Intrusion Detection Systems (IDS) are used to protect enterprises from attacks that exploit vulnerabilities in protocols permitted by the firewall security policy. There are multiple layers of IDS required to secure the enterprise—network based IDS and host based IDS. An intrusion detection system inspects the content of every packet traversing the network looking to detect signature based or anomaly based attacks. Once an attack is detected, the firewall is notified. The firewall immediately blocks the malicious traffic and reconfigures its policies to mitigate future attacks.

### Anti-Virus and Content Security

Viruses are the most publicized security threat due to their rapid propagation once systems are infected. Recent threats, such as Code Red and Nimda, underscore the need for an enterprise security strategy that encompasses multiple security technologies. Whereas, the firewall can provide the policy to allow/deny various types of content, additional security is needed to inspect the content and apply the content security policy. Anti-virus vendors integrate their engines with the firewall so that all content entering the enterprise network is scanned before being allowed in, ensuring protection on all platforms and layers in the network infrastructure via a single enforcement point.



Intelligent Security

Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Enterprises face content security threats from email and Internet usage that are not addressed by anti-virus technology. Content security systems like URL filtering and Instant Messaging filtering prevent inappropriate or restricted material from distribution into and within the organization. Anti-spam solutions help block unsolicited junk email from clogging email systems and wasting bandwidth and storage resources. Similar to anti-virus, other content security products are integrated with the firewall so that the objectionable content can be blocked at the gateway itself.

### Authentication and Authorization

Corporations use the Internet to provide selective resource access to remote employees, business partners, suppliers and customers. Authentication addresses the issue of identity management and there are many unique ways to identify users, partners, applications or transactions. A robust security infrastructure allows you to perform the appropriate authentication to the appropriate resource. Authorization then allows selective access to application resources based on policies. These applications can be integrated with the firewall to prevent the need to authenticate separately for access to each resource.

### Reporting and Monitoring

Audit logs are generated by every security application deployed in the network. These logs track network access and authentication, protocol usage and flag anomalies and unauthorized attempts to enter the enterprise network. Log data is also used to validate and fine-tune security policies and monitor the health of the security infrastructure. Integration with the firewall allows log files to be viewed centrally and events can be correlated to generate intelligent alerts and escalations.

### Performance and Availability

Network packets need to traverse several layers of security before they reach their destination. With increased network traffic and the need for deeper packet inspection at the firewall to block sophisticated intruders, overall system performance can be impacted. Performance acceleration technologies and high availability systems are required to ensure increased productivity and maximum uptime.

As described above, an enterprise has to deploy multiple security products to deliver a comprehensive security solution. Typical features on the list of must-haves are:

- Best-of-Breed Products—as no single vendor provides the best solution in every security category
- Single Policy Framework—to easily push policy to thousands of networks, systems, applications, and users instantly.
- Centralized Management—because a comprehensive solution is likely to include components from several security vendors.
- Support for Industry Standard Protocols—for seamless integration and interoperability

### Framework For Integrated Security Management

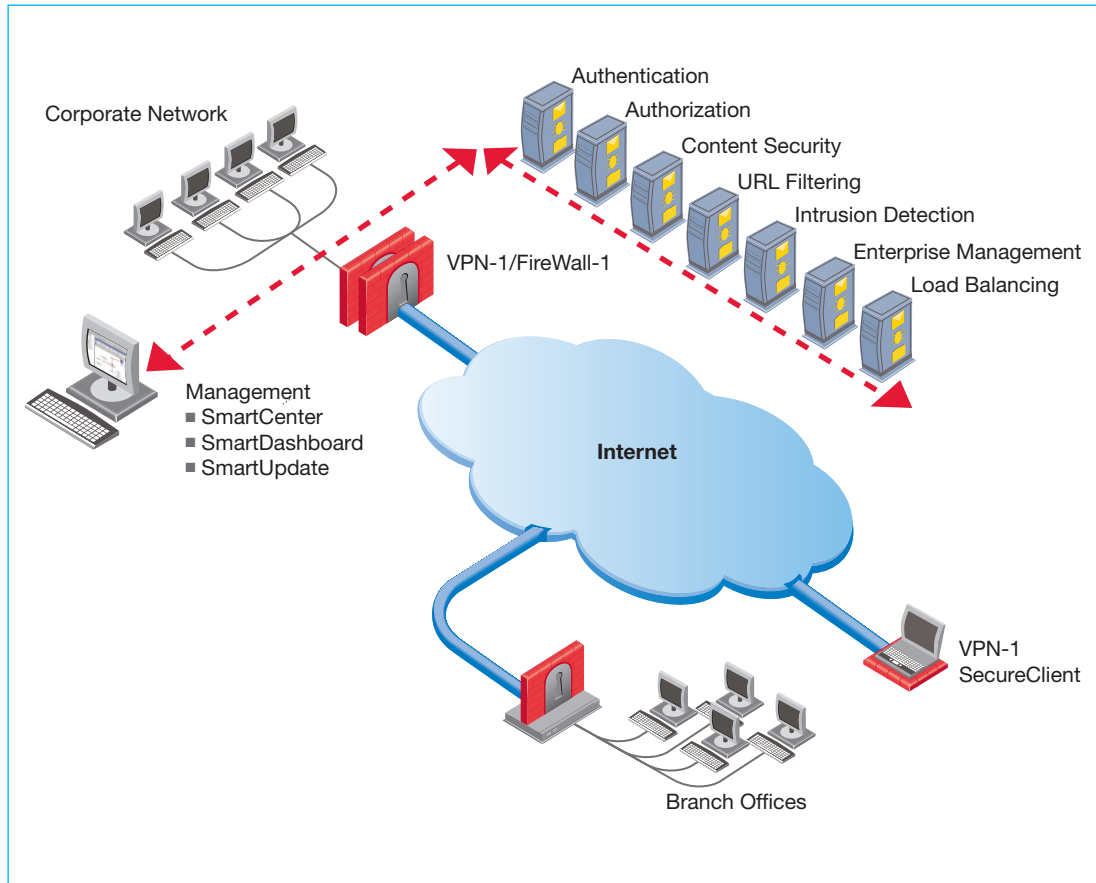
In 1997, Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for interoperability. Since then it has become the de-facto standard with its interfaces adopted by more vendors than any other security platform in the industry. OPSEC's wide range of integration interfaces addresses all areas of a complete Internet security architecture. With over 325 participating vendors and more than 175 certified products, the OPSEC framework guarantees customers the broadest choice of best-of-breed Internet security applications and deployment platforms—all of which are certified to interoperate as one integrated and centrally managed network security infrastructure. OPSEC solutions are available on a broad range of operating systems, including Linux, IPSO, Solaris, Windows, HP-UX and AIX, and offered by over 25 industry-leading hardware vendors.



Check Point  
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.



### OPSEC Integration Points

OPSEC provides a single integration framework via the OPSEC Software Development Kit (SDK) for multiple third-party products to integrate with Check Point VPN-1/FireWall-1. The SDK provides more than 20 time-tested interfaces that include industry-standard protocols and published Application Programming Interfaces (APIs).

Third party security products integrated into the Check Point security infrastructure are tested and “OPSEC-Certified” to guarantee seamless interoperability. By using “OPSEC-Certified” security products, enterprises can take full advantage of new security technologies and upgrade individual components without having to reconfigure the entire security infrastructure.

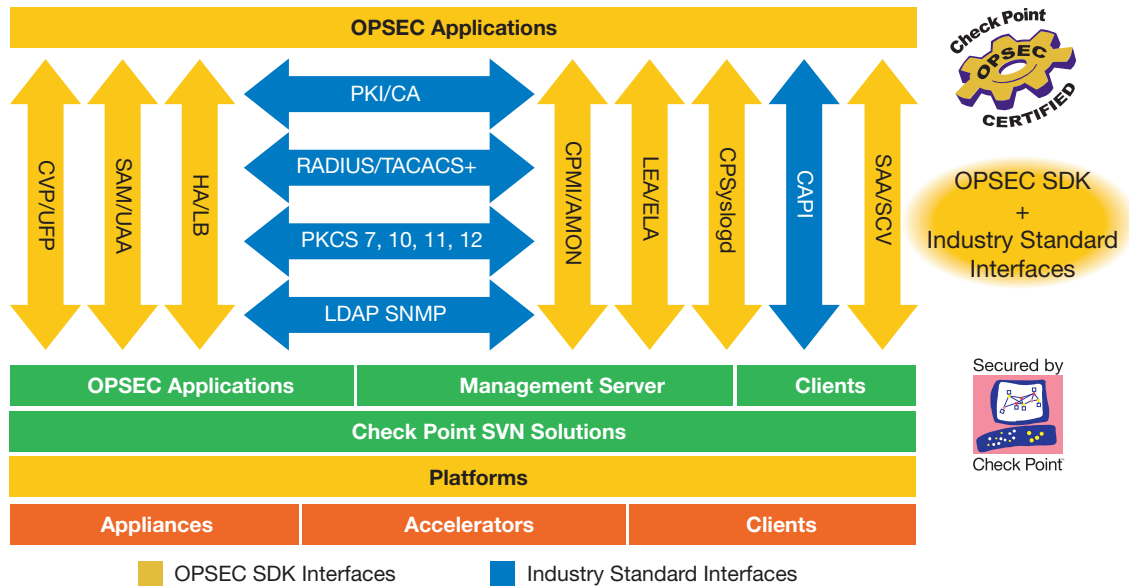
Under the “Secured by Check Point” program, Check Point Security solutions are delivered on a wide choice of hardware appliance platforms serving all market segments from consumers to small offices to enterprises and service providers.

These APIs, along with code samples, are available in the OPSEC Software Development Kit (SDK) to vendors and organizations who wish to integrate their products with the Check Point infrastructure.





The OPSEC APIs are comprehensive and leverage industry standard protocols.



The following table gives an overview of some of the OPSEC APIs.

API Name	Description	Function	Application Usage
CVP	Content Vectoring Protocol	Used to implement content validation and checking of messages and file or applet attachments	Content Inspection
UFP	URL Filtering Protocol	Used to enforce access control to external Web sites	URL filtering products
SAM	Suspicious Activity Monitoring	Used to enable third party applications to dynamically re-configure the firewall gateway	IDS
UAA	User Authority API	Used to create single authentication for user across applications	SSO
CPMI	Check Point Management Interface	Used to interface with Check Point object repository for centralized management	All applications

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

API Name	Description	Function	Application Usage
AMON	Application Monitoring	Used to monitor Check Point and third party applications	All applications
LEA	Log Export API	Used by external applications to retrieve real-time and historical log information	All applications
ELA	Event Logging API	Used by external applications to log events into the Check Point log database	All applications
SAA	Secure Authentication API	Used to integrate authentication devices & software to the VPN client	Authentication products
SCV	Secure Configuration Verification	Used to integrate desktop settings with enterprise FW/VPN	Remote access

## Benefits of the Check Point OPSEC Framework

### Comprehensive Security

Check Point's OPSEC security framework includes best-of-breed security partners and ensures centralized and consistent security enforcement across all security applications. By selecting among numerous OPSEC-certified applications, organizations can deploy a single comprehensive security infrastructure with the assurance that all components are guaranteed to optimally work together. Visit <http://www.opsec.com/solutions/index.html> to view a complete list of partner categories and certified solutions.

### Centralized Management

To facilitate simple and easy management, the OPSEC framework offers integrated multi-vendor security management directly from Check Point's SMART™ management console. Check Point's Smart OPSEC Manager, part of the SmartCenter family, dramatically lowers Total Cost of Ownership (TCO) by centralizing management and administration functions, specifically Policy Management, Security Provisioning and Incident Management for "OPSEC-Certified" applications.

### Policy Management

With so many devices and security products in the network, there is a critical need for centrally creating and managing security policies while enforcing these policies at multiple network points. Automating policy enforcement can dramatically reduce errors caused by human interfaces and interaction.

Today, using Check Point's SmartCenter, customers can manage their entire security policy across all OPSEC certified products. Check Point's centralized management architecture allows users to manage multi-vendor application operations and parameters from a single console, while leveraging vendor specific tools, which can be launched directly from SmartCenter.



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

This model of network security management helps in defining the best security practices for an enterprise and significantly lowers the risk of a security breakdown. This open approach provides a consistent single console for management, integrated parameters and management while retaining the full power of each vendor's unique capabilities and tools.

### ***Security Provisioning***

Security application deployment needs to be quick and seamless. As new applications are deployed, they need to be configured automatically and should have the ability to plug and play with the existing infrastructure.

Today, using SmartCenter™, administrators can quickly provision multiple “OPSEC-Certified” security applications with the ease of Check Point’s “One-Click” technology. “OPSEC-Certified” applications eliminate the need for manual configuration and enable plug-and-play with the security infrastructure.

With Security Provisioning, companies can have a centralized and streamlined deployment experience, saving time and reducing errors.

### ***Incident Management***

Identifying an attack, isolating the intrusion, responding quickly to the threat and preventing a recurrence is a challenge to most, if not all, corporations.

Today, Check Point’s SmartCenter imports and integrates event logs from “OPSEC- Certified” security applications and network devices and exports event logs to external management systems. In the future, security administrators will be able to automatically correlate events and generate real-time automated responses.

Being able to view and analyze consolidated security logs makes responding to an intrusion more manageable. In case of any abnormal activity, the policies and decisions can be quickly communicated to the enforcement points in real time.

### **Performance and Availability**

Firewalls as a gateway security product must be capable of handling multi-Gbps throughput common in most enterprises. Since every packet coming in from the public network has to be examined, the firewall cannot have any downtime. Through Check Point’s Next Generation™ (NG) SecureXL™ architecture, Check Point and OPSEC partners deliver seamless connectivity with multi-Gbps throughput and 99.999% availability. Log files generated by network devices and applications can be imported into the Check Point management console for performance and availability planning. Through the combined technology efforts of Check Point and OPSEC partners, OPSEC solutions are always at the forefront of performance and high availability.

### **OPSEC Can Significantly Lower Your Total Cost of Ownership**

Information security has become a key business enabler for enterprises to keep them more competitive and profitable. Successful deployments of a comprehensive security infrastructure include best of breed products from multiple vendors managed under a unified security architecture.

The OPSEC framework provides enterprises investment protection and significantly lowers the total cost of ownership (TCO) of deploying a comprehensive security infrastructure. The latest best of



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

breed solutions can be integrated into evolving hardware-based security platforms at a reduced TCO, without having to change the base infrastructure. Customers can build and grow their security infrastructures over time without the fear of obsolescence or interoperability.

**To Learn More About Building Comprehensive Security Solutions  
Visit Us At: [www.opsec.com](http://www.opsec.com)**

### 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. Check Point provides Intelligent Security Solutions for Perimeter, Internal and Web Security. Based on INSPECT, the most adaptive and intelligent inspection technology, and SMART Management, which provides the lowest TCO for managing a security infrastructure, Check Point's solutions are the most reliable and widely deployed worldwide. Check Point solutions are sold, integrated and serviced by a network of 1,900 certified partners in 86 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, 24 th Floor  
Ramat Gan 52520, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-575 9256  
e-mail: [info@CheckPoint.com](mailto:info@CheckPoint.com)

##### U.S. Headquarters:

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

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, and VPN-1 VSX are trademarks 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.

