



The NGX platform delivers a unified security architecture for Check Point perimeter, internal, and Web security.

Top 10 reasons to upgrade to the NGX platform

Take advantage of the NGX platform for more effective security

The NGX platform delivers new features and extended functionality to more than 20 Check Point solutions, offering stronger protection and smarter management to address the most challenging security problems. Critical new features offer deeper security, protecting more network and application types from more threats than any other solution. The NGX platform also unifies management across the four most critical layers of network security—perimeter, internal, Web, and endpoint. Simplified and powerful management features allow enterprises to manage even the most sophisticated networks more efficiently, with fewer resources, and lower total cost of ownership.

While there are hundreds of reasons to upgrade your Check Point products to NGX versions, listed below are the top 10 reasons why customers like you are taking advantage of the NGX platform for more effective security.

1. Increase security effectiveness by gaining control of perimeter, internal, Web, and endpoint defenses

A key prerequisite of effective security is ensuring policies and defenses are up-to-date without creating unnecessary administrative burden. Check Point enables this by allowing administrators to centrally manage Check Point gateways and endpoints—VPN-1® Pro™, Check Point Express™, Check Point Express CI, Check Point Integrity™, Connectra™, InterSpect™, VPN-1 Edge™, and VPN-1 VSX™—from a single console. In addition, the enhanced SmartUpdate™ feature provides administrators with clear visibility and control of new releases and available Hot Fixes.

2. Ensure confidentiality and availability of VoIP communications

The NGX platform gives VPN-1 Pro and Check Point Express gateways advanced security features to protect VoIP networks from threats such as call hijacking, call theft, network hacking, Denial of Service, and others to ensure confidentiality and availability of voice communications.

The most popular voice over Internet Protocol (VoIP) protocols and multiple networking configurations are supported, including application-layer filtering of H.323 v3/v4, MGCP, SCCP, and SIP packets to enable flexible VoIP networking configurations and solutions.

The NGX platform unifies management across the four most critical layers of network security—perimeter, internal, Web, and endpoint. Simplified, powerful management features allow enterprises to manage even the most sophisticated networks more efficiently, with fewer resources, and lower total cost of ownership.



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

3. Gain better insights into your network and security operations

SmartCenter™ and Provider-1® now provide centralized logging, tracking, monitoring, updating, and reporting for all Check Point solutions, providing users with a unified view of log data for better understanding of the status of their network and security deployments. Eventia Reporter™ captures Integrity event data—as well as data from all Check Point solutions—providing administrators and chief Internet security officers with end-to-end visibility and automated reports to validate and audit security effectiveness.

4. Ensure consistent and comprehensive defense updates against new threats

A new SmartDefense™ Services console provides administrators with the ability to universally update security configurations and defenses from one, unified interface. By having a single location for all SmartDefense Services, deployment of security updates is streamlined and it enables administrators to quickly ensure that defenses for Connectra, InterSpect, and VPN-1 are consistent and comprehensive. In addition, global SmartDefense updates for Provider-1 enable service providers and large enterprises to easily push policy updates to end users.

SmartDefense now provides better protections for an increased number of protocols, including DCE-RPC, DNS, email, multicast and unicast routing, and peer-to-peer. For example, administrators now have more control at a lower level of granularity over MSN Messenger functions such as application sharing, file transfers, and whiteboarding.

5. Enable unified threat management for branch offices and midsize businesses

Organizations can now efficiently increase security at branch offices or throughout midsize businesses by deploying VPN-1 Express CI gateways or VPN-1 Edge integrated security appliances and using SmartCenter to centrally manage the whole security policy. With integrated firewall, VPN, intrusion prevention, and antivirus, these solutions take advantage of Check Point's unified security architecture for delivering intelligent security solutions across organizations of any size without increasing management costs.

6. Simplify VPN deployment in distributed environments

Administrators can quickly establish VPNs between sites with rapidly changing infrastructures by using the route-based VPN capabilities of VPN-1 Pro. Combined with support for dynamic routing protocols such as OSPF, VPN-1 Pro makes it simple to provision stable, reliable service across distributed environments.

7. Quickly, easily extend remote access for employees

The SSL Network Extender™ Web applet now enables administrators to quickly and easily provide secure remote access without installing remote-access clients on end-user machines. This browser-based solution can be managed centrally from within SmartCenter and is integrated with Integrity Clientless Security to ensure that only safe PCs are allowed access to the network, protecting them and your critical network resources from remote threats.

8. Protect Web applications from advanced hacking techniques

Web Intelligence™ enables companies to better protect Web servers against increasingly complex and aggressive attacks—including buffer overflows, SQL injections, cross-site scripting attacks, and more—by using Web Intelligence capabilities that are tightly integrated into VPN-1 Pro and Connectra gateways. Also, Web Intelligence has been expanded to protect against new attacks such as LDAP injections and to conceal Web server error messages from users, thwarting reconnaissance efforts by hackers and ensuring the confidentiality and integrity of business data.

9. Support multicast applications across a distributed environment

Organizations can now encrypt multicast applications such as video and audio conferencing through VPN-1, enabling the secure distribution of content to all locations. Administrators can also restrict access to multicast traffic to specific groups, ensuring that multicast applications are not inadvertently broadcast to unauthorized or outside groups.

10. Extend visibility of security administration to technical support staff and auditors

SmartPortal™ is a Web-based GUI for SmartCenter that provides a read-only view of an organization's security policy, enabling nonadministrative users to troubleshoot security issues without the danger of changing policies or security rules. Now, internal teams can work together seamlessly in mitigating attacks and troubleshooting network and security issues—without compromising security policy.

Learn more about the Check Point NGX platform

Find out how you can take advantage of these top 10 reasons and hundreds more by visiting the NGX Upgrade Center at <http://www.checkpoint.com/ngx>, where you will find important information, tools, and resources to make upgrading your Check Point products to the NGX platform simple and easy.

©2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo 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, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

March 29, 2006 P/N 502113

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
www.checkpoint.com



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.