



Endpoint Security

Check Point Endpoint Security is a single agent for endpoint security.





Check Point Endpoint Security

Single agent for endpoint security

Check Point Endpoint Security™ is the first single agent for total endpoint security that combines the highest-rated firewall, network access control (NAC), program control, antivirus, anti-spyware, data security, and remote access. It protects PCs and eliminates the need to deploy and manage multiple agents, reducing total cost of ownership. Check Point Endpoint Security is the only solution that includes both data security to prevent data loss and theft and a VPN client for secure remote communications.

PRODUCT BENEFITS

- Single agent for all your endpoint security needs
- Easy to deploy, easy to manage
- Eliminates the need to manage multiple security agents
- Erases compatibility issues with separate agents
- Reduces administration time and effort
- Lowers total cost of ownership

 Firewall/NAC/Program Control	Protects endpoint systems by restricting both inbound and outbound traffic, ensuring that they are in a secure state before allowing access to the network and automatically enforcing policies on which programs are allowed to run on PCs.
 Antivirus/Anti-spyware	Detects and removes viruses, spyware, and other malware based on a combination of signatures, behavior blockers, and heuristic analysis, featuring the highest detection rates and hourly signature updates through the SmartDefense™ update service. Based on the award-winning ZoneAlarm® Internet Security Suite.
 Data Security	Provides data protection on laptops, PCs, and removable media via a strong and efficient blend of full-disk encryption, access control, port management, and removable media encryption. Based on market-leading Pointsec® technologies.
 Remote Access	Enables secure remote access to end users by encrypting and authenticating data transmitted during remote access sessions between the endpoint and corporate network.

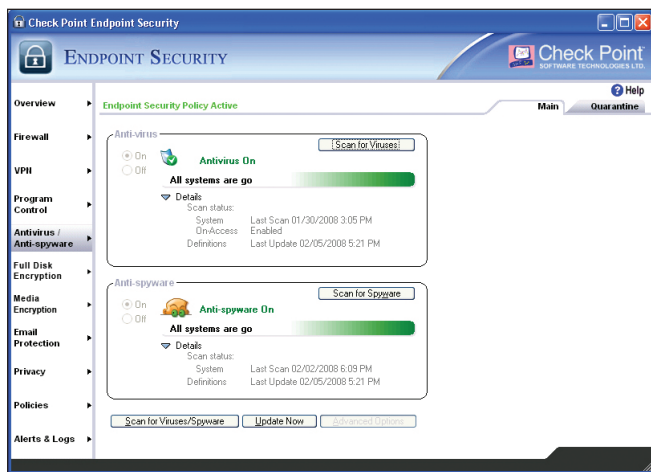
NGX™

The NGX platform delivers a unified security architecture for Check Point.

SINGLE AGENT FOR ENDPOINT SECURITY

Check Point Endpoint Security™ is the first single agent for endpoint security that combines the highest-rated firewall, network access control (NAC), program control, antivirus, anti-spyware, data security, and remote access. This enables security administrators to deploy endpoint security with a single installation and reduce the number of software updates that need to be tested and deployed.

- Easy deployment via single installation process
- Streamlined system performance requiring minimal memory and CPU resources
- Transparent to end users, requiring no user interaction to keep systems updated and secure



Best-of-breed endpoint security technologies in a single agent that's easy to deploy.

Highest-rated, award-winning firewall

Check Point Endpoint Security features an industry-leading firewall that blocks unwanted traffic, prevents malware from infecting endpoint systems, and makes endpoints invisible to hackers.

- Uses “stealth mode” to make endpoints invisible to hackers scanning for vulnerable systems
- Controls which applications are allowed network access
- Ensures that approved programs cannot be spoofed, tampered with, or hijacked

Unique Program Advisor

Program Advisor makes implementing program control easy and effective. It leverages a Check Point knowledge base of hundreds of thousands of trustworthy applications and suspected malware—updated in real time—to automatically ensure that only legitimate and approved programs are allowed to run on PCs.

- Automatically kills the execution of malicious programs
- Enables administrators to automate most application policy decisions, saving valuable administration time

Broadest malware protection

Check Point Endpoint Security terminates viruses, spyware, keystroke loggers, Trojans, rootkits, and other malicious programs before they can damage endpoint systems. Backed by the industry's fastest security update services.

- Comprehensive antivirus, anti-spyware, and host intrusion prevention
- Hourly updates provide immediate protection against the latest malware

Remote access

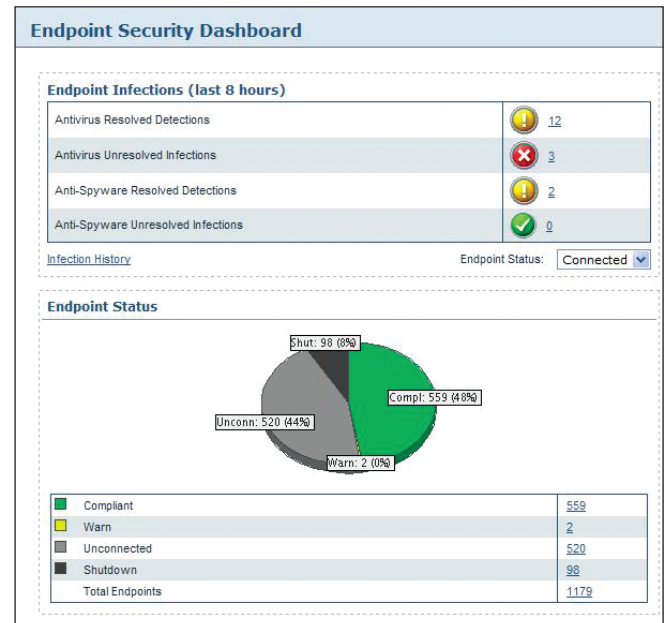
Only Check Point Endpoint Security unifies advanced remote access as an indispensable part of endpoint security.

- IPSec VPN client based on the award-winning VPN-1® SecureClient™
- Includes flexible connectivity options and supports multiple authentication schemes
- Applies full security policies to remote access traffic

Market-leading data security

Check Point Endpoint Security includes market-leading data security based on Pointsec technology to provide data protection through an efficient blend of full-disk encryption, access control, port management, and removable media encryption.

- Full-disk encryption provides the most complete and comprehensive protection for all data
- Keeps data safe by controlling activity on ports and devices
- Encrypts sensitive data transferred via portable media devices such as USB storage devices and CDs and DVDs



A single management console centralizes policy management across all essential endpoint security functions reducing complexity, time, and effort.

Policy compliance and NAC

Prior to granting network access to any user, Check Point Endpoint Security enforces a comprehensive NAC policy to ensure that each endpoint is current with the latest antivirus, critical patches, service packs, and applications such as browsers and VPN agents.

- Ensures only safe endpoint devices can access the network
- Easy to configure NAC for both remote access and internal network access
- Support for industry-standard 802.1x authentication enables NAC in multi-vendor networking environments

SINGLE CONSOLE FOR SIMPLIFIED MANAGEMENT

Check Point Endpoint Security features a powerful, unified management system that reduces overall cost and complexity

by enabling administrators to deploy, manage, and monitor security policy for thousands of endpoints across a distributed organization—all from a single console. The management server installs in minutes, and the agent software can be deployed quickly without end-user involvement. It also provides powerful tools to enhance and customize endpoint security policies specific to the needs of an organization and enables distinct policies to be applied automatically to endpoints as they change networks, locations, and access points.

- Monitor, analyze, and report on security events from a single administrative console
- Easy to deploy and manage with one simple installation
- Unified with Check Point SMART management to enable monitoring, analysis, and reporting of endpoint security events from SmartCenter™, Provider-1®, and Eventia® management systems

PRODUCT SPECIFICATIONS

Protection details	
Firewall	
Firewall rules	• Block/allow traffic based on packet data, source/destination locations, protocols, ports, and time activities occur
Zone rules	• Restrict/allow network activity based on traffic origination or destination zone: Trusted Zone, Blocked Zone, Internet Zone • Allow/deny traffic based on security locations: Host, site, IP address, IP range, IP subnet and mask
Hot spot registration	• Allows for a temporary, controlled opening in the policy, regardless of the policy restrictions, so that the user may register to a local hot spot
Program control	
Program control	• Limits exposure to vulnerabilities and attacks by restricting network access on a per-program basis • Moderates network access for programs • Uses program permissions applied to individual programs or program groups to control program activity
Program permissions	• Sets permissions for individual programs or group of programs: Allow, block, ask, terminate
Program authentication	• Verifies programs have not been tampered with by authenticating via MD5 signature or signed certificates
Program Advisor	• Automatically terminates known malicious programs • Automates application policy decisions based on real-time data collected from millions of PCs worldwide
Program groups	• Sets program permissions for groups of programs rather than for individual programs
Network access control (NAC)	
Endpoint policy compliance and auto remediation	• Corrects policy violations: Antivirus, anti-spyware, firewall rules, software patches, specific application versions, registry entries • Quarantines unsafe PCs and automatically brings endpoints into compliance • Restricts network access from unknown guest users
Cooperative Enforcement®	• Ensures endpoint computers remotely connecting to the network are running an agent, have a specific policy, comply with enforcement rules in the security policy assigned • Restricts or terminates network access for noncompliant endpoints
Network segmentation-level NAC	• Cooperative Enforcement with VPN-1 gateways
Port-level NAC	• 802.1x authentication support, third-party switch and wireless access point support • Restricts noncompliant endpoints to isolated VLAN: Limited to specific destination IP, ports, and protocols
VPN NAC	• Supported gateways: VPN-1, Connectra™, and VPN gateways from Cisco Systems and Nortel Networks • Enforces spyware checks, keylogger removal, and ensures antivirus and operating system patches are current • VPN NAC on Connectra: includes on-demand browser-based solution for session confidentiality, disables spyware on guest PCs before granting SSL VPN access
Antivirus	
Heuristic virus scan	• Scans files and identifies infections based on behavioral characteristic of viruses
On-access virus scan	• Scans files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses
Deep scan	• Runs a detailed scan of every file on selected scan targets
Scan target drives	• Specifies directories and file types to scan
Scan exclusions	• Specifies directories and file extensions not to be scanned
Treatment options	• Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete
Third-party antivirus support	• McAfee VirusScan, Symantec Norton Antivirus, Trend Micro PC-cillin/OfficeScan, Sophos Anti-virus, Computer Associates eTrust InoculateIT, Computer Associates VET, Check Point Endpoint Security Antivirus, Kaspersky Antivirus, NOD32 Antivirus, AVG Antivirus, AVAST Antivirus, BitDefender Antivirus, F-Secure Antivirus, Panda Antivirus, Microsoft OneCare Antivirus

Continued on page 4

PRODUCT SPECIFICATIONS (CONTINUED)

Protection details	
Anti-spyware	
Intelligent quick scan	• Checks the most common areas of the file system and registry for traces of spyware
Full-system scan	• Scans local file folders and specific file types
Deep-inspection scan	• Scans every byte of data on the computer
Scan target drives	• Specifies which directories and file types to scan
Scan exclusions	• Specifies directories and file extensions not to be scanned
Treatment options	• Enables choice of action agents should take upon detection of virus: Automatic, notify, or confirm
Data security	
Preboot authentication	• Native logon credentials and customized background
Full-disk encryption	• Encrypts all defined hard-drive volumes including partition boot records, operating system, system files, user data
Authentication and login methods	• Authentication and login methods: User ID/password, tokens, smartcards, Single Sign-On, Windows Integrated Login
Multiple platform support	• Windows (including Vista), Macintosh, and Linux
Centralized management	<ul style="list-style-type: none"> • Remote Help: For password resets • Disk Recovery: Automatic creation of centrally stored recovery file for disaster recovery • Active Directory Integration: User password synchronization with Windows • Centralized Policy Configuration: Integration with third-party forensics and recovery tools (e.g., Win PE)
Media and port protection	<ul style="list-style-type: none"> • Complete port and removable media management • Unique media authorization • Offline access to encrypted media • Transparent removable media encryption • Extensive auditing alerts <ul style="list-style-type: none"> • Whitelist and blacklist • Microsoft and Novell support and third-party certifications • Kernel mode technology and anti-tampering features • Active Directory integration
Remote access: IPSec VPN	
Connectivity options	• Dynamic and fixed IP addressing for dialup, cable modem, and DSL connections
Authentication	• Preshared secrets, X.509 digital certificates, SecurID, username and password, RADIUS, TACACS, Check Point Internal Certificate Authority (ICA)
High availability and load sharing	• Inbound VPN connections distributed across a cluster of VPN-1 gateways, multiple entry points
Multiple connectivity modes	• Office Mode, Visitor Mode, Hub Mode
Management	
Single management console	<ul style="list-style-type: none"> • For policy configuration, policy administration, reporting, and analysis • Web-based administrator console
Role-based administration	<ul style="list-style-type: none"> • Creates administrator accounts limited to specific user sets • Assigns an administrator to specific entities—user catalogs or groups • Creates accounts that are allowed only to perform specific functions
Unified with Check Point SMART Management	<ul style="list-style-type: none"> • Manage endpoint security events from SmartCenter • Centralizes security event management and reporting via Eventia Analyzer and Eventia Reporter • Enables shared management server, login, console, log viewing, and event management
Management server log monitoring	• SNMP trap, Syslog

MANAGEMENT

Operating systems*	<ul style="list-style-type: none"> • Windows Server 2003 • Check Point SecurePlatform™
Browsers	<ul style="list-style-type: none"> • Internet Explorer 6 (SP2) and 7 • Mozilla Firefox 1.5 and higher

AGENT

Operating systems*	<ul style="list-style-type: none"> • Windows XP Pro (SP2) • Windows 2000 Pro (SP4)
Certifications	<ul style="list-style-type: none"> • Common Criteria Evaluation Assurance Level 4 (EAL4)

* New editions of Check Point Endpoint Security will be made available in Q2 2008. Please contact a Check Point representative for details.

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, 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

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.