



CHECK POINT ENDPOINT SECURITY FIREWALL & COMPLIANCE

ENDPOINT SECURITY FIREWALL & COMPLIANCE

Controls in and outbound traffic and ensures policy compliance

Product Benefits

- Control inbound and outbound traffic along with policy compliance
- Centrally definable traffic control, security levels and stealth technology
- Verify that endpoints meet the organizational security policy. Prevent non-compliant devices to access sensitive resource, and transparently remediate such devices.
- Knowledge base of more than one million trusted or suspicious programs

Product Features

- The desktop firewall protects the integrity of endpoints by regulating inbound and outbound traffic
- Compliance scanning ensures endpoint systems are compliant with corporate security policy
- Application control ensures only legitimate, approved programs are allowed to run and perform tasks on endpoints. Unapproved Applications and untrusted Applications can be blocked or terminated.

OVERVIEW

Attackers are continuing to find new ways to compromise endpoint systems. The best corporate firewalls cannot stop all malicious inbound and outbound traffic, especially when a user is not always working within a corporate network. Providing endpoints with firewalls can be a logistical nightmare due to the scale of deployment, lack of centralized control, and logging capabilities.

SOLUTION

Check Point Endpoint Security Firewall & Compliance protects endpoints by controlling inbound and outbound traffic and ensuring policy compliance, with centralized management from a single console. Desktop Firewall policies protect endpoint systems from unauthorized access. Integrated stealth technology makes endpoints invisible to attackers.

We guard against network worms, malware, unauthorized access and attacks from suspicious sources. Unique to Check Point firewall, stealth technology makes endpoint systems invisible to attackers. Finally, providing unified security options in a single management console and server make enforcement and monitoring of incidences easier.

DESKTOP FIREWALL

The desktop firewall protects the integrity of endpoints by regulating inbound and outbound traffic. Definable zones and security levels prevent malware from infecting endpoint systems, block targeted attacks and stop unwanted traffic. Stealth technology makes endpoints invisible to potential attackers.

COMPLIANCE CHECK

Compliance Check scans endpoint systems for compliance with corporate security policy. Systems failing compliance can be directed to remediation.

Administrators can ensure that endpoints are compliant in a number of different areas including:

- Endpoint Security Client software is up-to-date
- Endpoint has the latest authorized Operating System Service Packs
- Check for “blacklisted” applications either running or existing on endpoint
- Check for authorized anti-malware software, versions and DAT updates.

APPLICATION CONTROL

Application control ensures that only legitimate and approved programs are allowed to run and perform tasks on endpoints. Program authenticity is verified to prevent spoofing, altering or hijacking of applications. Application Control automatically creates an inventory of all applications attempting network access, and blocks unauthorized connections and data transfers by malicious programs.

REMOTE ACCESS VPN

Check Point Remote Access VPN is included in the Access Control Software Package along with Firewall & Compliance. This provides users with secure, seamless access to corporate networks and resources when traveling or working remotely. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data.

COMPLETE ENDPOINT SECURITY

Endpoint Security Access Control is fully integrated into our endpoint security suite, saving time and reducing costs by allowing customers to quickly expand security protection while keeping a single client and simple user experience to meet changing requirements.

Complete Endpoint Security Solution	
Data Security	
Full Disk Encryption	✓
Media Encryption	✓
Port Control	✓
Capsule Docs	✓
Access Control	
Firewall	✓
Application Control	✓
Compliance	✓
Remote Access VPN	✓
Threat Prevention	
Antivirus	✓
SandBlast Agent Threat Emulation	✓
SandBlast Agent Threat Extraction	✓
SandBlast Agent Anti-Bot	✓
SandBlast Agent Forensics	✓

CENTRAL MANAGEMENT

Endpoint Firewall and Compliance Check is centrally managed, enabling central policy administration, enforcement and logging from a single, user-friendly console. Centralized management offers unmatched leverage and control of security policies.

SPECIFICATIONS

COMPLIANCE CHECK	
Verify Programs	Verify if a certain program is running or not running on the endpoint device
Verify Files	Verify if a certain file exists or does not exist on the endpoint device
Verify Registry Keys	Verify if a specific registry key and value is set or not set on the device
Verify Anti Malware Solution and Virus Signature Age	Supported vendors: Check Point, Symantec, McAfee, Trend Micro, Kaspersky, Nod32, AVG, Avast, Sophos, Panda CA, Inoculate IT engine, BitDefender, MS Forefront
Restricted Policy	Ability to enforce a dedicated security policy for non-compliant endpoints
Remediation	Ability to automatically remediate non-compliant endpoints

See SecureKnowledge [SK102150](#) for more specifications.

ORDERING ACCESS CONTROL

PACKAGE	SKU
Access Control	CPEP-ACCESS-1Y CPEP-ACCESS-RENEWAL-1Y CPEP-ACCESS-P

TRY ENDPOINT SECURITY TODAY

Reduce your security gaps with unified monitoring, management, and enforcement of endpoint security. [Get started with a trial today](#), and learn more about our complete [Endpoint Security solution](#).

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com